STI 10-036

A Tutorial on Probabilistic Risk Assessment and its Role in Risk-informed Decision Making

Presented at
Eighth Space Systems Risk Management Symposium
April 6, 2010
The Aerospace Corporation, El Segundo, CA

Homayoon Dezfuli, Ph.D.
NASA System Safety Technical Fellow

ACKNOWLEGEMENTS

The material and examples in this tutorial are derived from the following sources:

- ***NASA PRA Procedures Guide; Version 1.1, August 2002***
  http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf
- ***NASA PRA Training Modules***
- ***NASA Risk-informed Decision Making Handbook (Draft)***

Outline

- Preamble
- A Typical Risk Management Process
- The Concept of Risk-informed Decision Making (NASA's Perspective)
- Some Key Concepts
- Probabilistic Risk assessment (PRA) Overview
- PRA Methodology Synopsis
- PRA Results of a Real Space System
- Summary

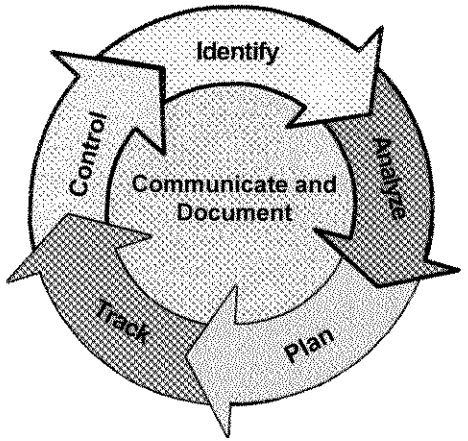
Preamble

- **Probabilistic Risk Assessment is a tool that can inform decisions during the entire lifecycle of a program/project**
  - **Risk analysis of decision alternatives in light of programmatic objectives (to support direction setting decisions)**
  - **Risk analysis of selected alternatives to set priorities (to support risk management decisions)**
- **Probabilistic Risk Assessment can play a major role in**
  - **Design decisions and**
  - **Operation decisions**

A Typical Risk Management Process

A Typical Risk Management (RM) Process

- Identify – *Identify* program risk "issues"
- Analyze – Estimate the likelihood and consequence components of the risk issues
- Plan – *Plan* the *Track* and *Control* actions
- Track – *Track* and compile the necessary risk data, measuring how the RM process is progressing
- Control – Determine the appropriate *Control* action, execute the decision linked to that action, and verify its effectiveness
- Communicate and Document –communicating and documenting all risk information throughout each program phase

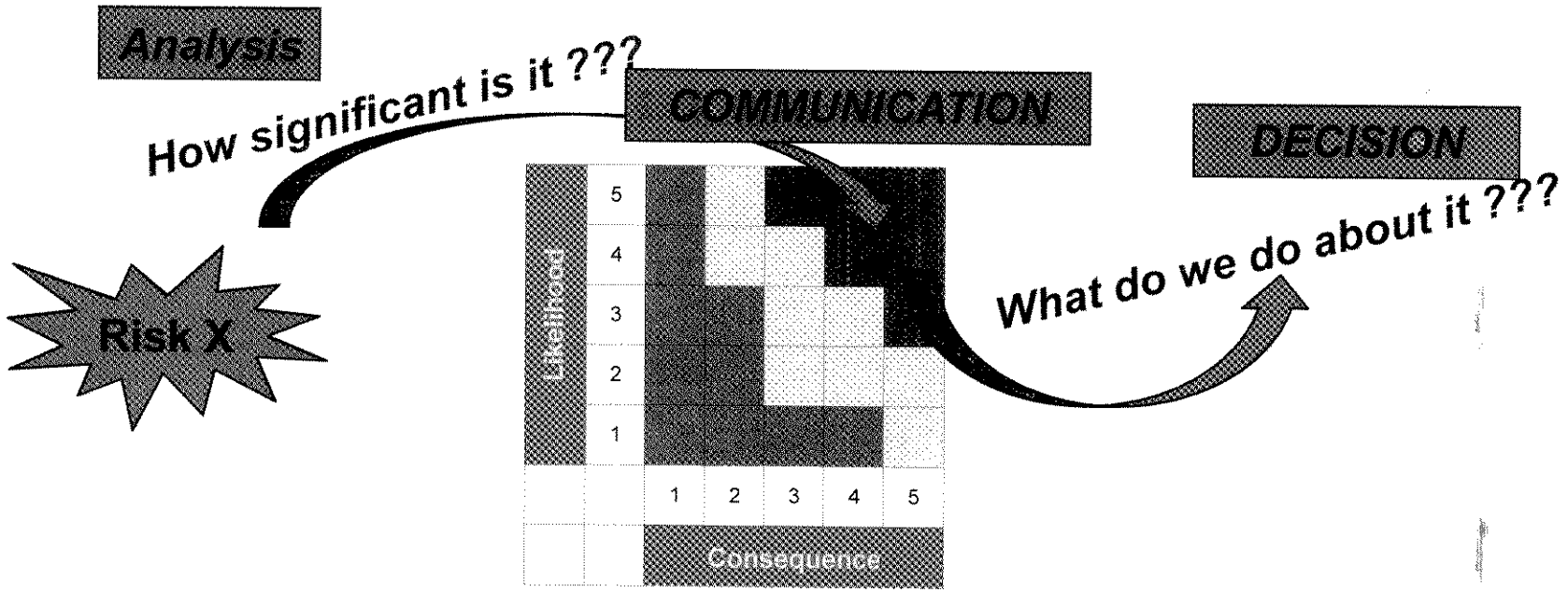


Emphasis on

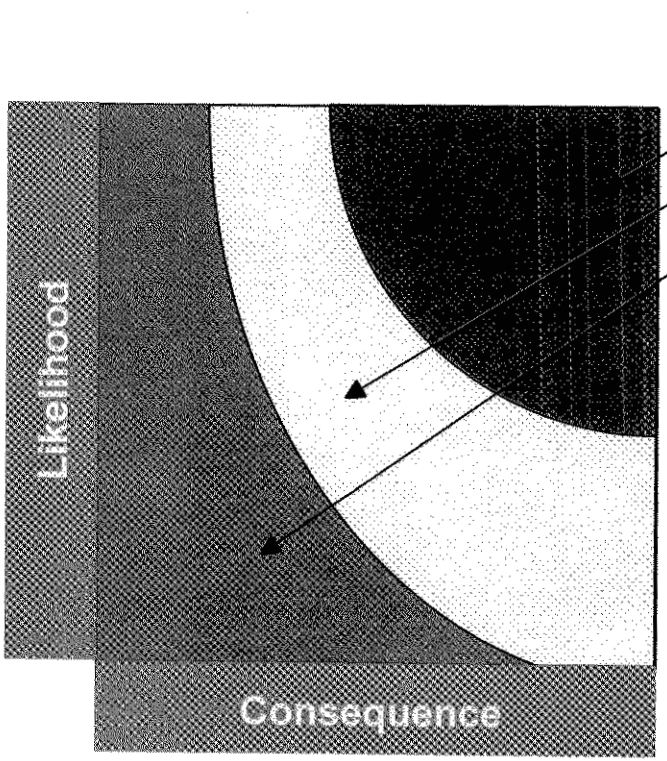
- **"management" of individual "risks"**
- **monitoring and accountability for action items associated with "risks"**

A Typical Risk Management Process (Cont.)

- **Relies heavily on the application of risk matrices**
- **Risk "issues" are mapped onto the matrix individually**



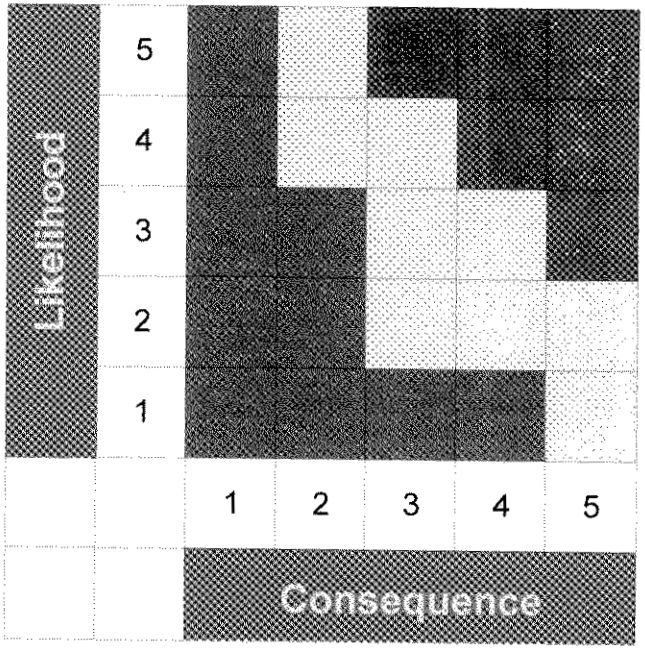
Origin of Risk Matrix



Red >> High Risk
Yellow >> Medium Risk
Green >> Low Risk

Iso-Risk (Equal Risk) Curves

Risk Matrix Derived from Iso-Risk Curves



Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Cautionary Notes on the Use of Risk Matrix

- A tool for communicating among cognizant and responsible entities
- Presents summary information about the results of an analysis or assessment of particular risks, and places those results in the context of previously established action thresholds
- The purpose of this communication is to coordinate the organizational risk management response
  - Which risks most urgently need management attention?
  - What risks are being elevated?
  - What risks are under control?
- The risk matrix does not add new technical content to the discussion that should occur anyway. It only provides a familiar vehicle for conveying that content. It is not an analysis tool: it is a tool that promotes efficiency in communication.

Cautionary Notes on the Use of Risk Matrix (Cont.)

- Risks are displayed on a risk matrix in order to frame a discussion of the appropriate current risk management response to those risks
- Traditionally, this has been done by color-coding the cells of the risk matrix, with "red" calling for significant attention, "green" implying that things are under control, and "yellow" in between.
- The thresholds separating different-colored regions are necessarily specific to programs and organizations
  - Risk tolerance is different among different programs
  - Priorities are different among different programs
- Therefore, the likelihood and consequence scales must be specific to the organizational and program context in which a given risk matrix is being used
  - They must be defined unambigously

Risk-Informing Decisions Making

(Based on NPR 8000.4A)

History of "Risk-Informed"

- **Evolved in the mid-1990's at Nuclear Regulatory Commission in the context of nuclear plant [safety] risk**
- **Formulation of "risk-informed" may have been a reaction to overzealous advocacy of risk-based regulation: aggressively modifying [admittedly inefficient] traditional approaches to regulation, based on risk model results**

What is Risk-Informed Decision Making (RIDM)?

- **A risk-informed decision-making process that uses a diverse set of performance measures (some of which are model-based risk metrics) along with other considerations within a *deliberative* process to inform decision making.** ***Paragraph A.14 of NASA NPR 8000.4A***

  Note to Paragraph A.14: A decision-making process relying primarily on a narrow set of model-based risk metrics would be considered "risk-based."

- **Decisions are informed by an integrated risk perspective rather than being informed by a set of individual "risk" contributions whose cumulative significance is not understood**

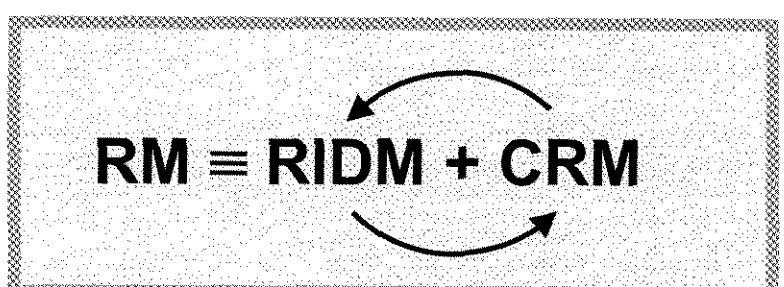
How Does RIDM Help?

- **RIDM is a structured process aimed at achieving success by proactively risk-informing the selection of decision alternatives.**
- **RIDM tries to foster development of the most robust technical basis for decision-making**
  - **Couples the attributes of the proposed decision alternatives to the objectives that define success;**
  - **Considers all attributes of significance to the stakeholders in an integrated manner: technical, safety, schedule and cost;**
  - **Helps ensure that a broad spectrum of decision alternatives are considered;**
  - **Involves quantitative assessment of the merits and drawbacks of each proposed decision alternative relative to the stated objectives;**
  - **Accounts for the uncertainties inherent to each proposed decision alternative to the extent that they impact the achievement of the stated objectives; and**
  - **Communicates the quantitative assessment of the proposed decision alternatives into the decision environment, where it is deliberated along with other considerations to form a comprehensive, risk-informed basis for alternative selection**
    - **Deliberative process intended to capitalize on tacit organizational knowledge after the analysis / modeling stage**

NPR 8000.4A

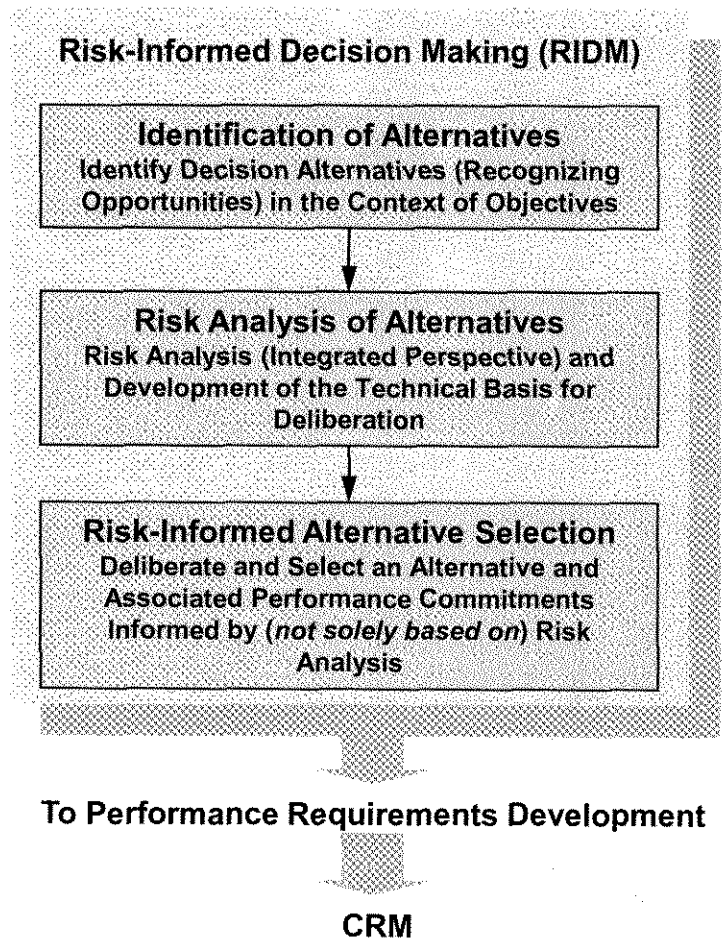
- **The latest version of NPR 8000.4A, Agency Risk Management Procedural Requirements, was issued on December 16, 2008**
  - Accessible from NASA Online Directives System (NODIS) Library
  - http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8000&s=4A
- **This directive evolves NASA's Risk Management (RM) approach to entail two complementary processes:**
  - Risk-informed Decision Making (RIDM)
    - Emphasizes the proper use of risk analysis in its broadest sense to make risk informed decisions that impact all mission execution domains (e.g., safety, technical, cost, and schedule)
    - Formulates recommendations for performance requirements
  - Continuous Risk Management (CRM)

    Focuses on the management of risk associated with implementation of baseline performance requirements

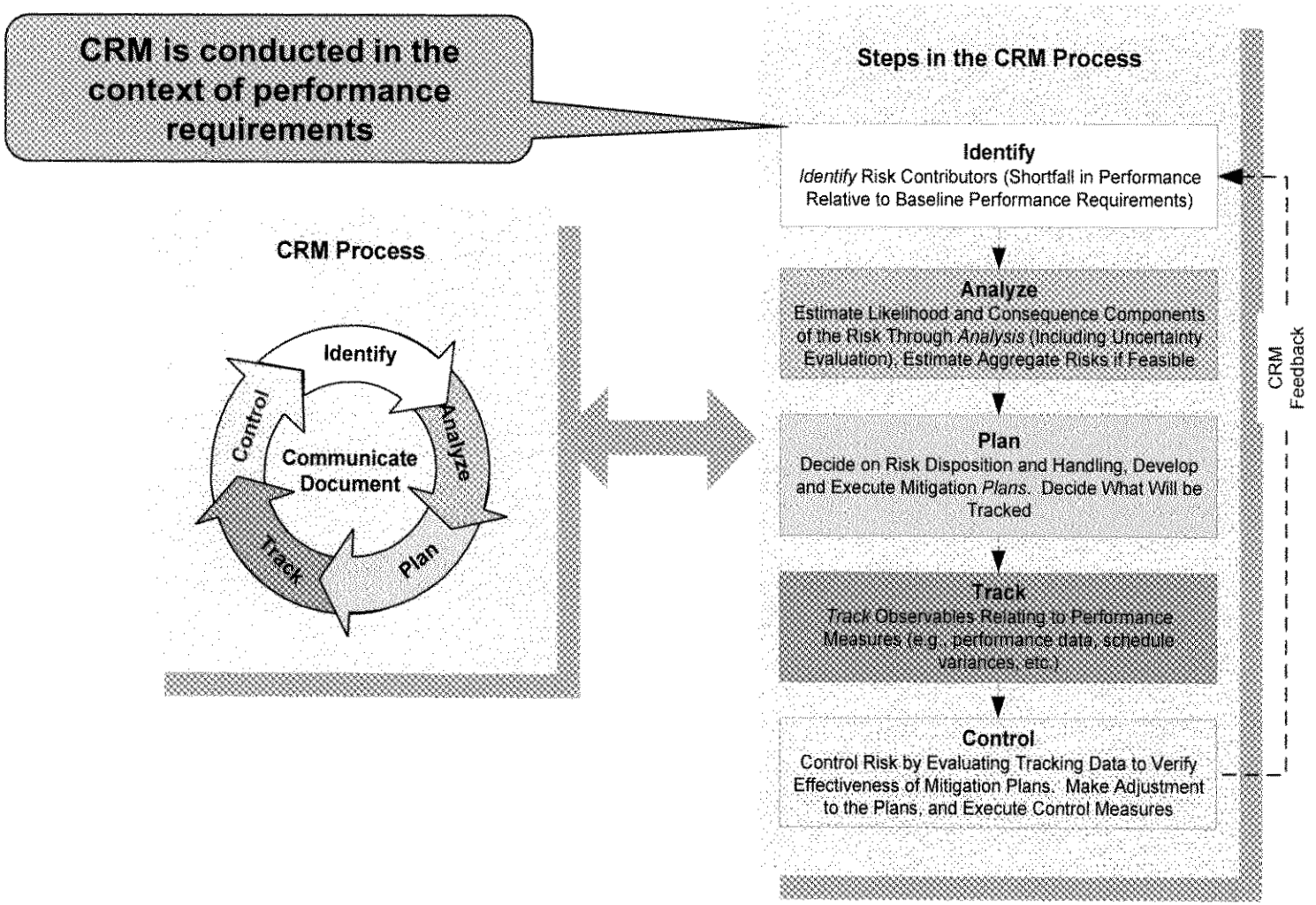


The RIDM Process

- **Identification of decision alternatives (*decision context*) and considering a sufficient number and diversity of Performance Measures**
- ***Risk analysis* of decision alternatives (uncertainty analysis of performance associated with the alternative**
- ***Selection* of a decision alternative *informed by* (not solely based on) *Risk Analysis Results***



The Continuous Risk Management (CRM) Process



Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Key Terms and Concepts Important to RIDM

Performance Measures and Performance Objectives

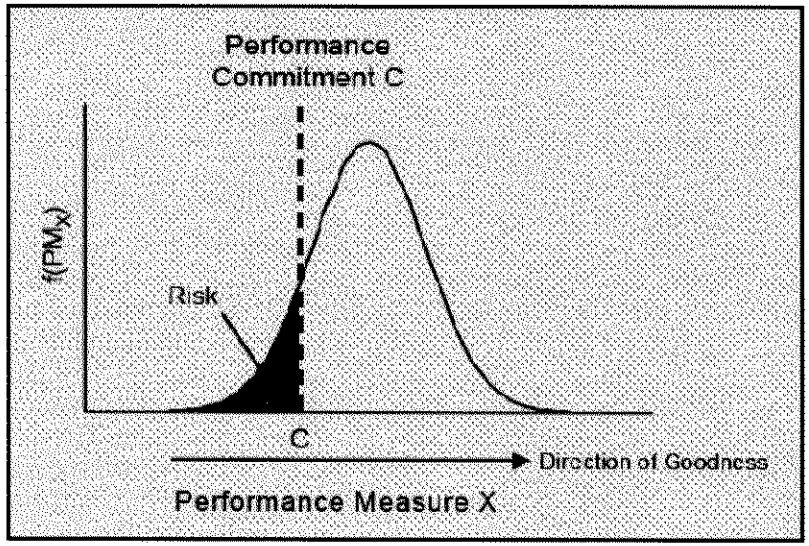
- **A Performance Measure is a metric used to quantify the extent to which a Performance Objective is fulfilled**
  - **Safety** (e.g., avoidance of injury, fatality, or destruction of key assets)
  - **Technical** (e.g., increase thrust or output, maximize amount of observational data acquired)
  - **Cost** (e.g., execution within minimum cost)
  - **Schedule** (e.g., meeting milestones)
- **Examples of Performance Objectives and corresponding Performance Measures**
  - **Maintain Astronaut Health** → **Probability of Loss of Crew (P(LOC))**
  - **Minimize Cost** → **Cost ($)**
  - **Maximize Payload Capability** → **Payload Capability (kg)**
  - **Maximize Public Support** → **Public Support (1 – 5)**
- **An Imposed Constraint is a limit on the allowable values of the Performance Measure with which it is associated**
  - **Example: A hard limit on minimum acceptable payload capability**

Definition of Risk

- The term "risk", when used without further qualifications, is very general and applies to a large variety of user contexts
- In general, risk is uncertainty regarding the future outcome of an undertaking of some kind: a decision alternative, a project, a launch, etc.
- In the context of mission execution, risk is the expression of the potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly, established and stated performance requirements
  - The performance shortfalls may be related to any one or more of the following mission execution domains:
    - Safety
    - Technical performance
    - Cost
    - Schedule

Performance Commitment and its Relationship to Risk

- **A performance commitment is a performance measure value set at a specified percentile of the performance measure's pdf**

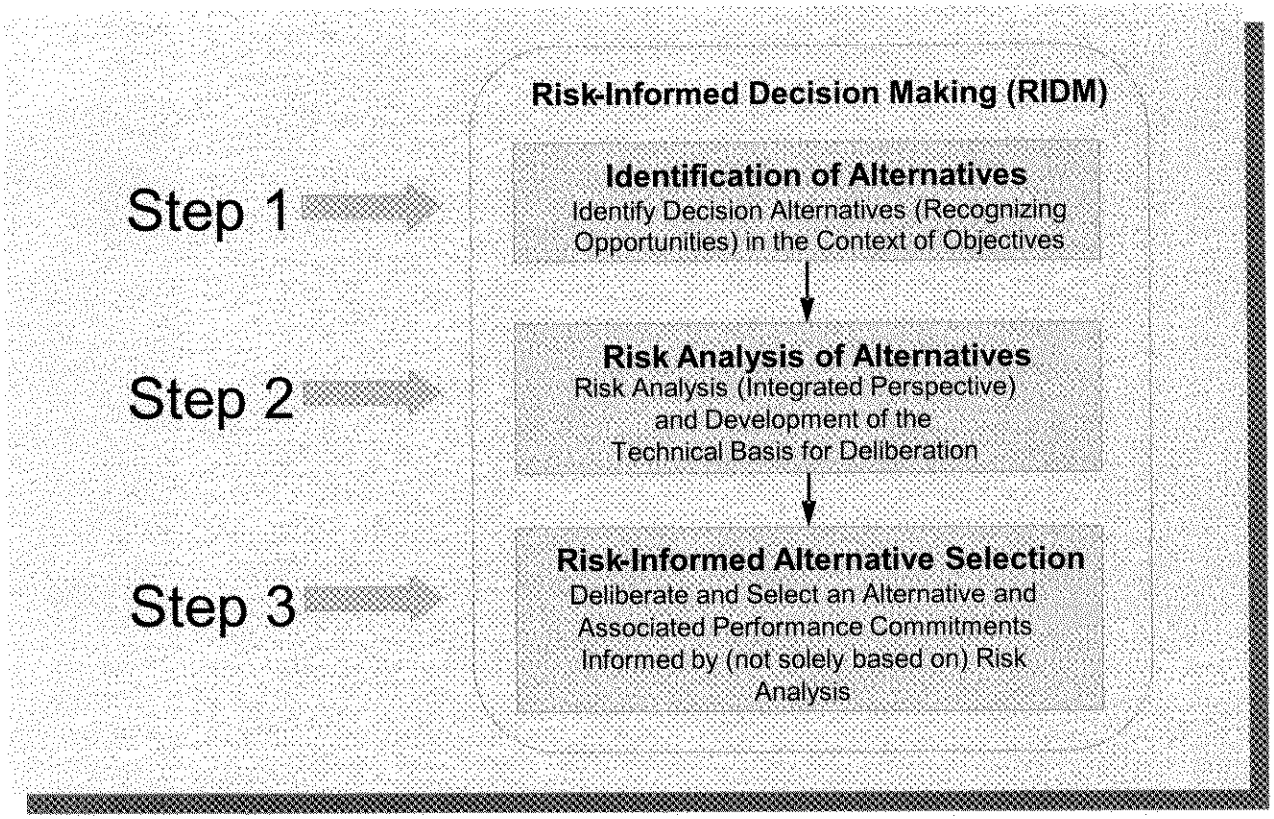


Operational Definition of Risk

- **The "triplet" concept of "risk" is *operationally* useful for defining, analyzing, and managing risk**
  - **The *scenario(s)* leading to degraded performance with respect to one or more Performance Measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage);**
  - **The *likelihood(s)* of those scenario(s); and**
  - **The *consequence(s)* (severity of the performance degradation) that would result if the scenario(s) was (were) to occur**

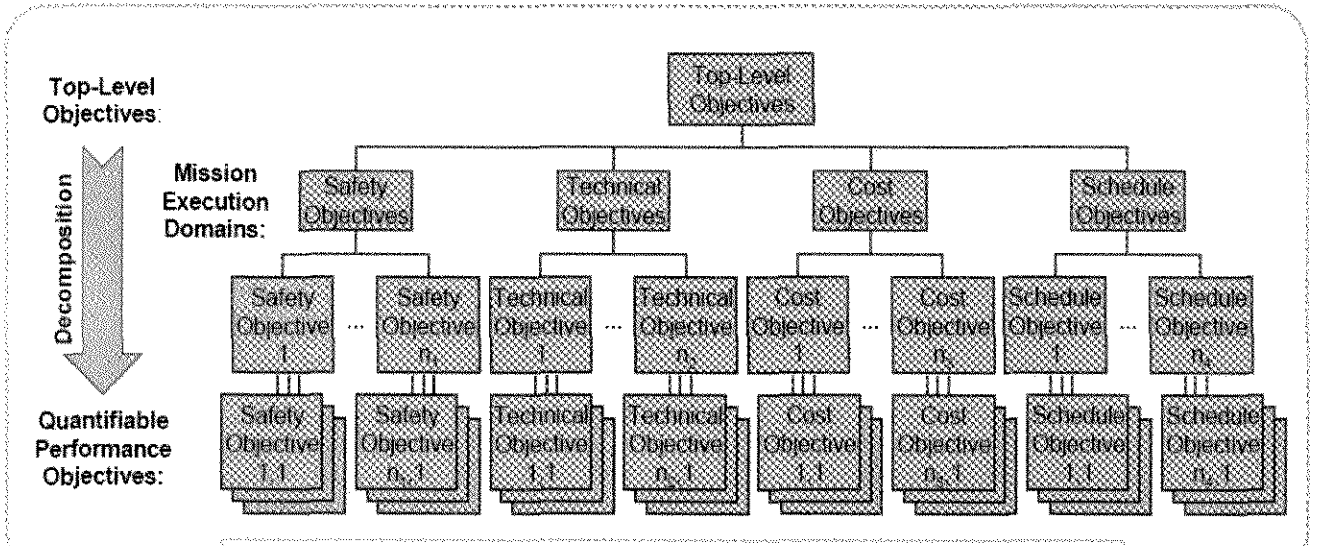
The RIDM Process

RIDM Process Steps



RIDM Process – Step 1
Derive Performance Measures from Objectives

- **In general, it can be difficult to assess decision alternatives against multifaceted and/or qualitative top-level objectives**
- **To deal with this situation, objectives are decomposed, using an objectives hierarchy (OH), into a set of lower-level performance objectives that any attractive alternative should have**
- **A performance measure is then developed for each performance objective, as the quantity that measures the extent to which a decision alternative meets the performance objective**



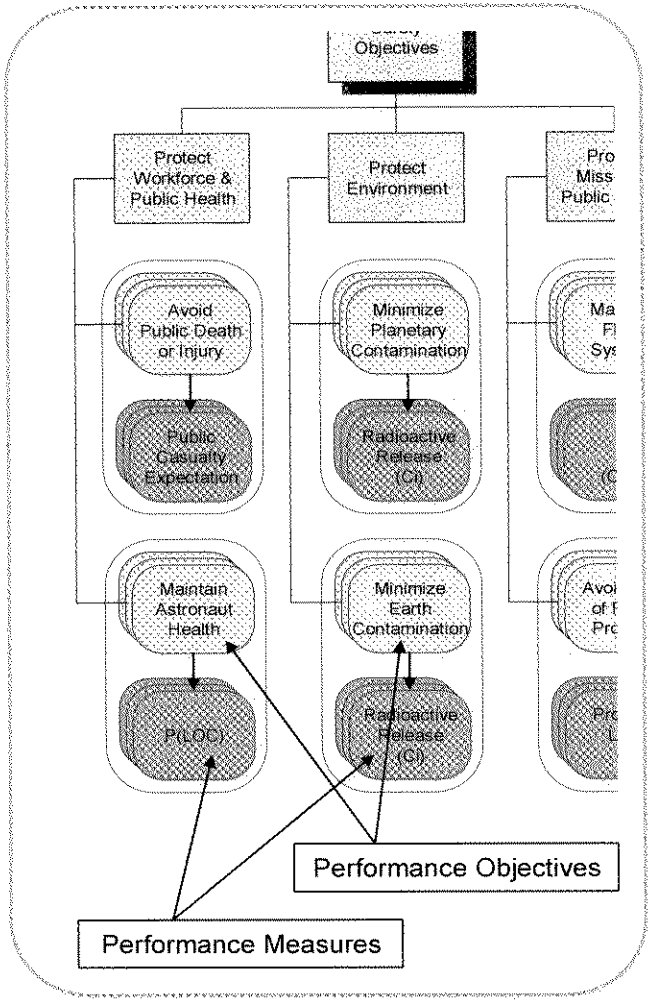
Notional Objectives Hierarchy

Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

RIDM Process – Step 1

Derive Performance Measures from Objectives (cont.)

- **Objectives are decomposed into quantifiable Performance Measures**
- **Some Performance Measures may have *Imposed Constraints***
- **Some Performance Measures are unconstrained but have a desirable direction of goodness**



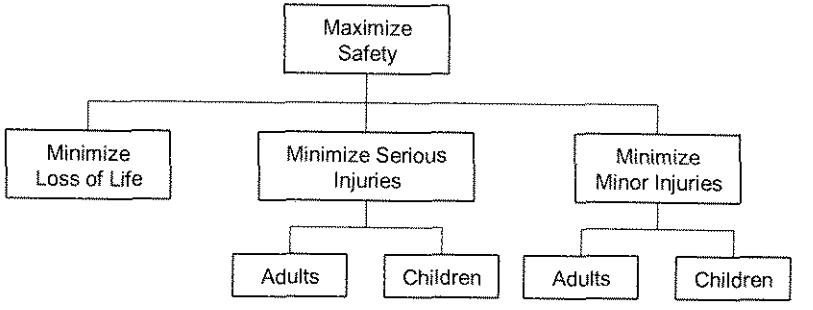
RIDM Process – Step 1
How is OH Different from Means Objectives?

Objectives Hierarchy

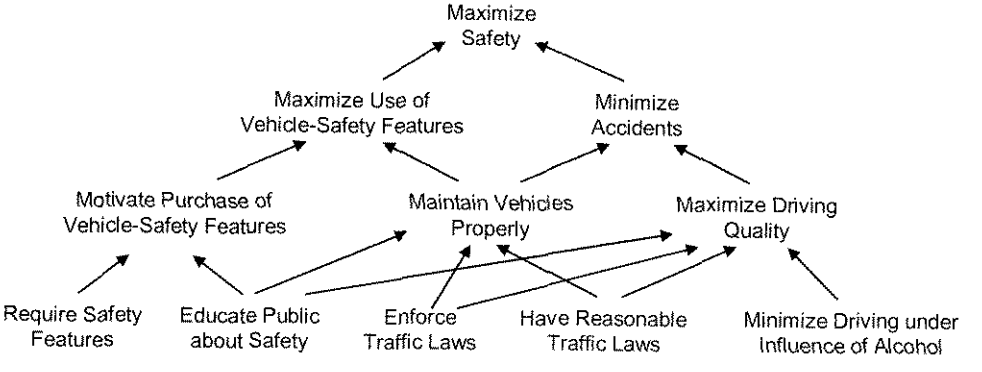
- Explain what is meant by the higher-level objective
- Partition the higher-level objective into its constituent parts
- Don't impose a solution;
- Are structured in a hierarchy

Means Objectives Network

- Are ways of accomplishing higher-level objectives
- May relate to multiple higher-level objectives;
- Imply a solution;
- Are structured in a network



(Fundamental) Objectives Hierarchy

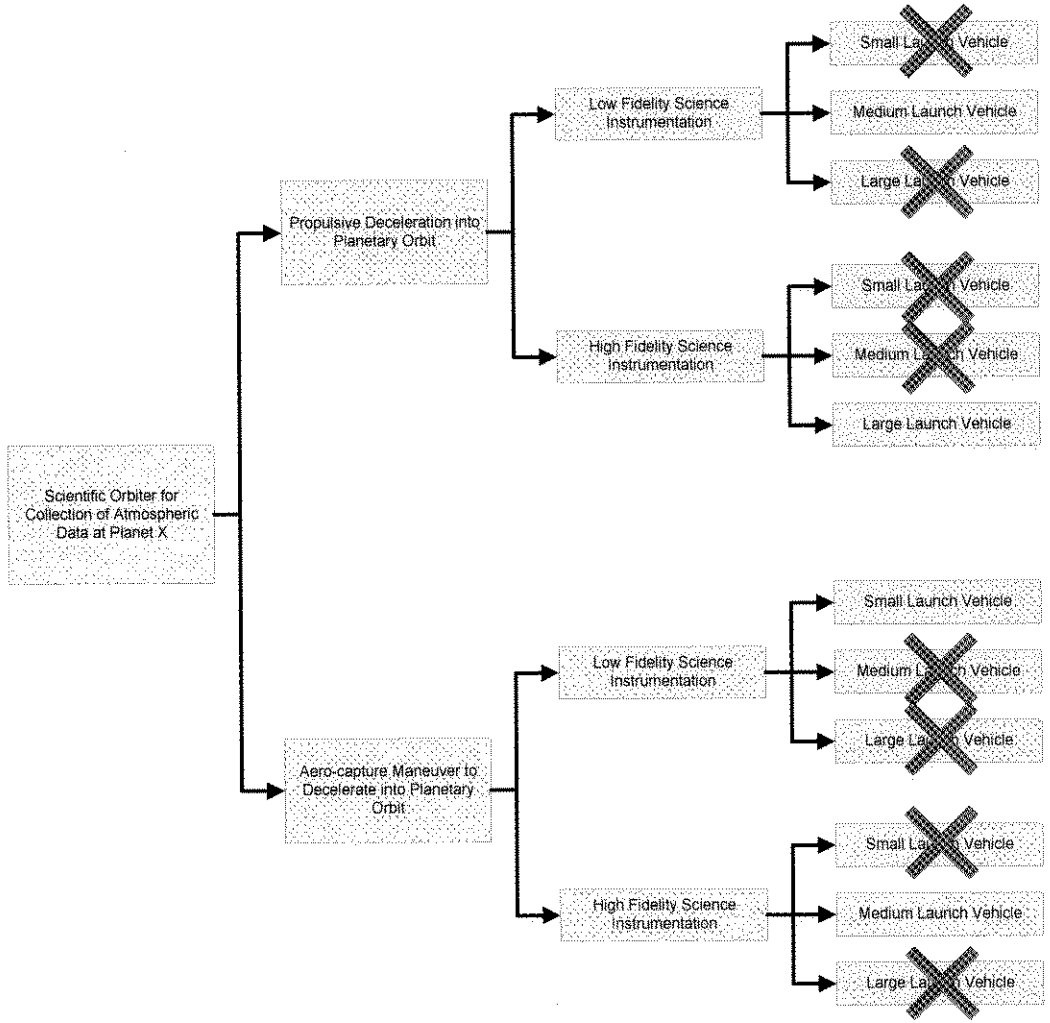


Means Objectives Network

RIDM Process – Step 1
Compiling Alternatives

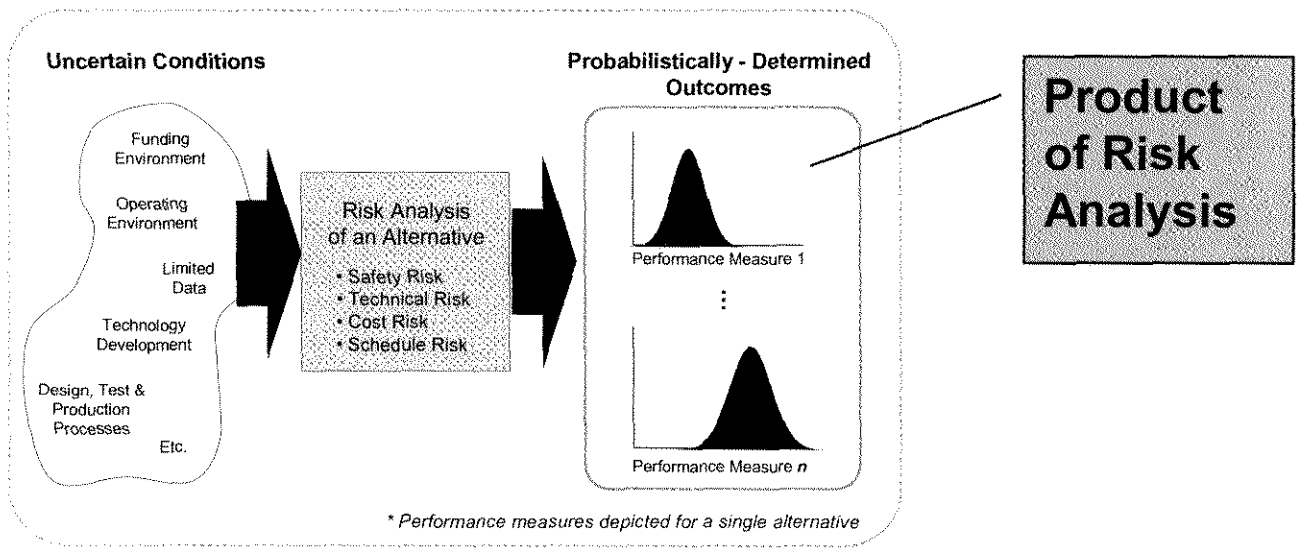
Alternative design solutions are generated as part of the Systems Engineering process

Low-fidelity feasibility assessment (e.g., first-order analysis, engineering judgment) is used to prune the trade tree and narrow the set of alternatives to analyze further



RIDM Process – Step 2
Risk Analysis of Alternatives

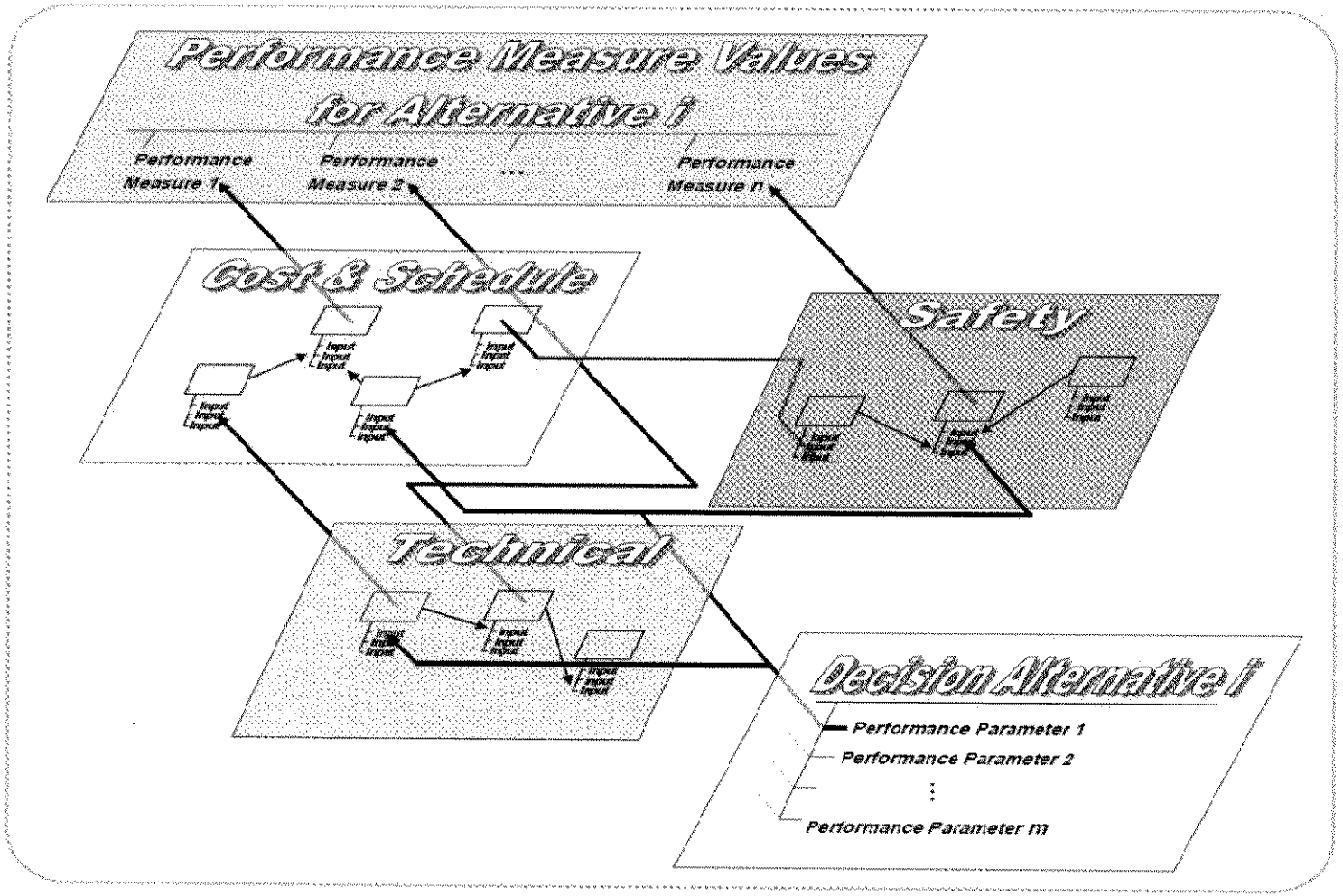
- **Goal: to develop a risk analysis framework that integrates domain-specific performance assessments and quantifies the performance measures**
  - **Risk Analysis** - probabilistic modeling of performance



- **The challenge is to establish a transparent framework that:**
  - Operates on a common set of performance parameters for each alternative
  - Consistently addresses uncertainties across mission execution domains and across alternatives
  - Preserves correlations between performance measures

RIDM Process – Step 2
Risk Analysis of Alternatives (cont.)

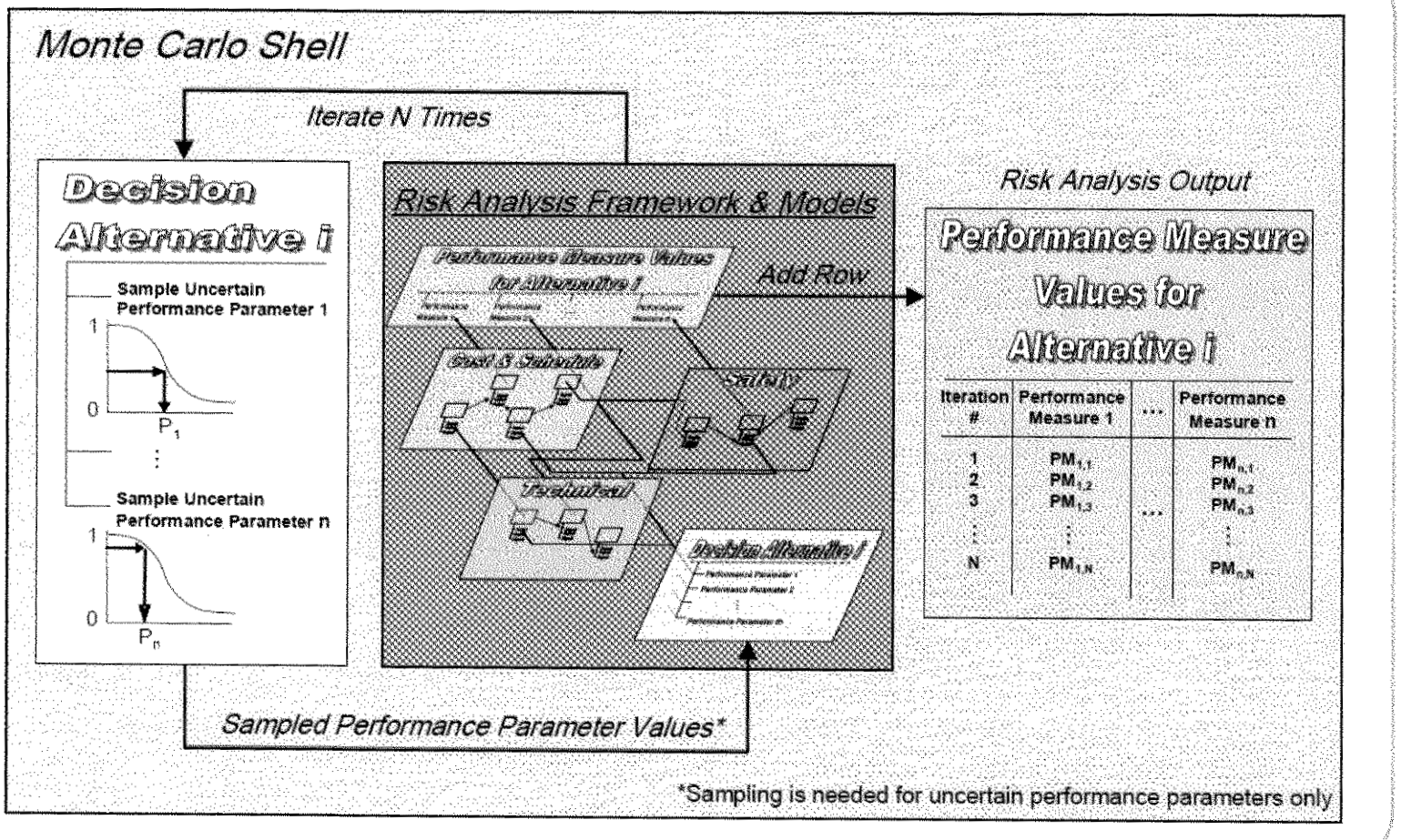
- **Setting the risk analysis framework (alternative specific)**



RIDM Process – Step 2

Risk Analysis of Alternatives (cont.)

- **Quantification via probabilistic modeling of performance**



Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

RIDM Process – Step 2

Choosing the analysis methodologies

- Detailed domain-specific analysis guidance is available in domain-specific guidance documents like the ***NASA Cost Estimating Handbook***, the ***NASA Systems Engineering Handbook***, and the ***NASA Probabilistic Risk Assessment Procedures Guide***

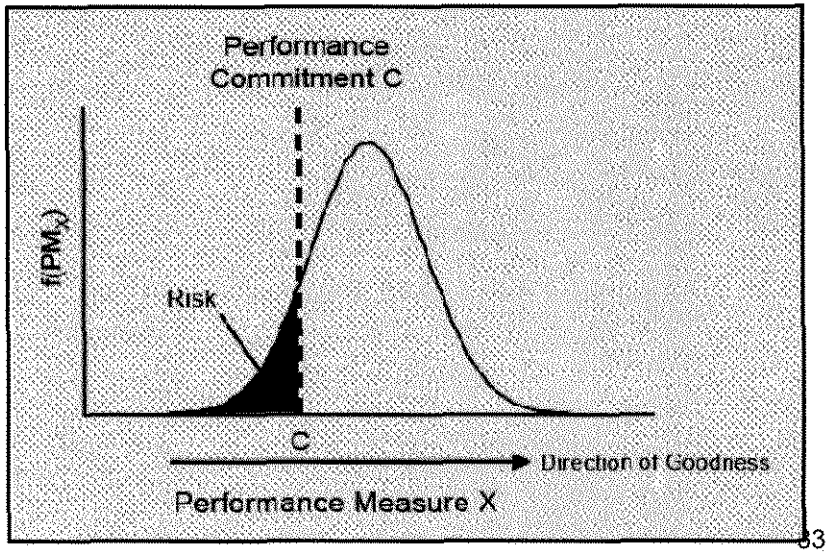
- Depending on project scale, life cycle phase, etc., different levels of analysis are appropriate. The rigor of analysis should be enough to:
  - Assess compliance with imposed constraints
  - Distinguish between alternatives

- Iteration is to be expected as part of the analysis process, as analyses are refined and additional issues are raised during deliberations

RIDM Process – Step 3

Comparing Alternatives in Terms of Candidate Performance Commitments

- **Performance Commitments**
  - A **performance commitment** is a performance measure value set at a specified percentile of the performance measure's pdf
  - Performance commitments help to anchor the decision-maker's perspective to specific performance expectations for each alternative
  - For a given performance measure, the performance commitment is set at the same percentile for all decision alternatives
  - Performance commitments support a **risk-normalized** comparison of decision alternatives, at a level of **risk tolerance** determined by the decision maker

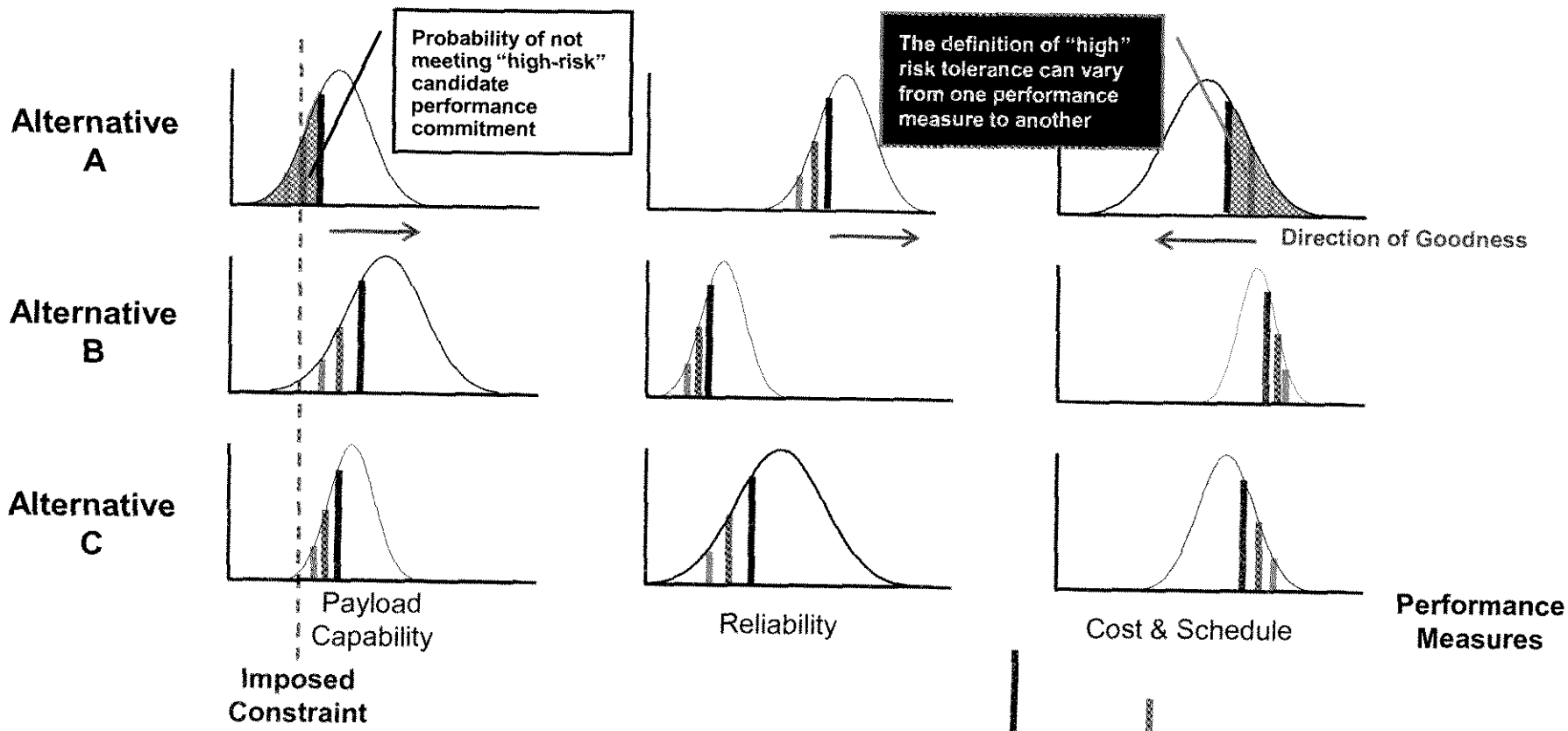


RIDM Process – Step 3

Develop Risk-Normalized Candidate Performance Commitments

Risk Analysis is Conducted on Alternatives A, B and C → **Set PM Ordering and Candidate PM Risk Tolerances** → **Candidate Performance Commitments defined at Candidate PM Risk Tolerances**

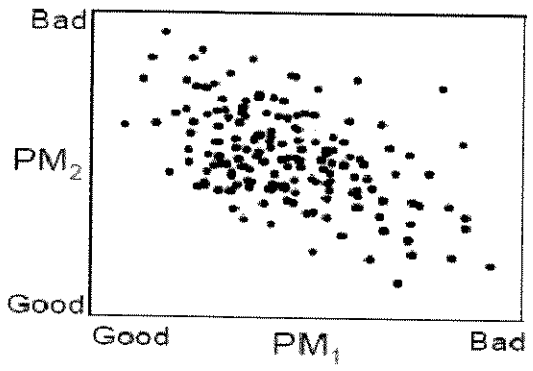
Candidate Performance Commitments facilitate comparison of performance across a range of risk tolerances



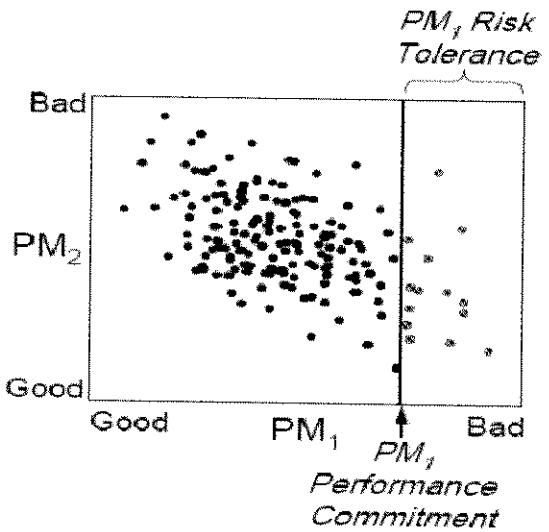
Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

RIDM Process – Part 3

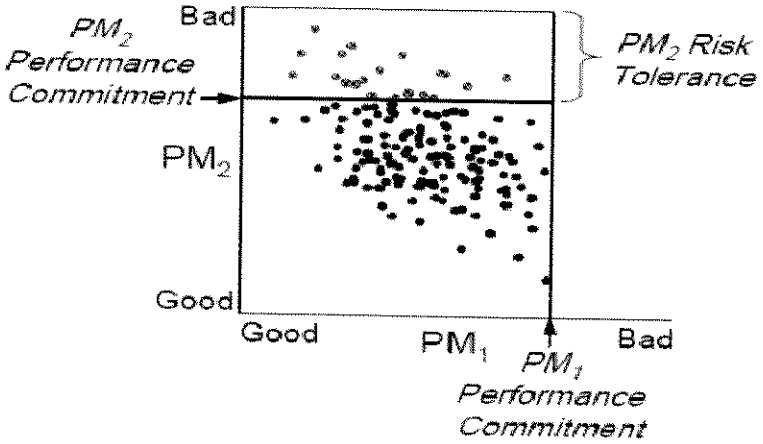
Performance Commitments are to be Developed in a Conditional Fashion



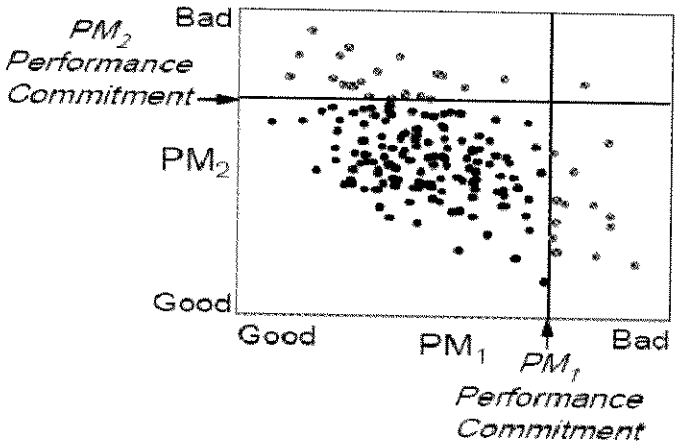
a. Risk analysis output for Alternative i



b. PM_1 performance commitment set at the specified risk tolerance



c. PM_2 performance commitment set at the specified risk tolerance, given compliance with PM_1 performance commitment



d. Performance commitments for PM_1 and PM_2, given the specified PM risk tolerances and PM ordering

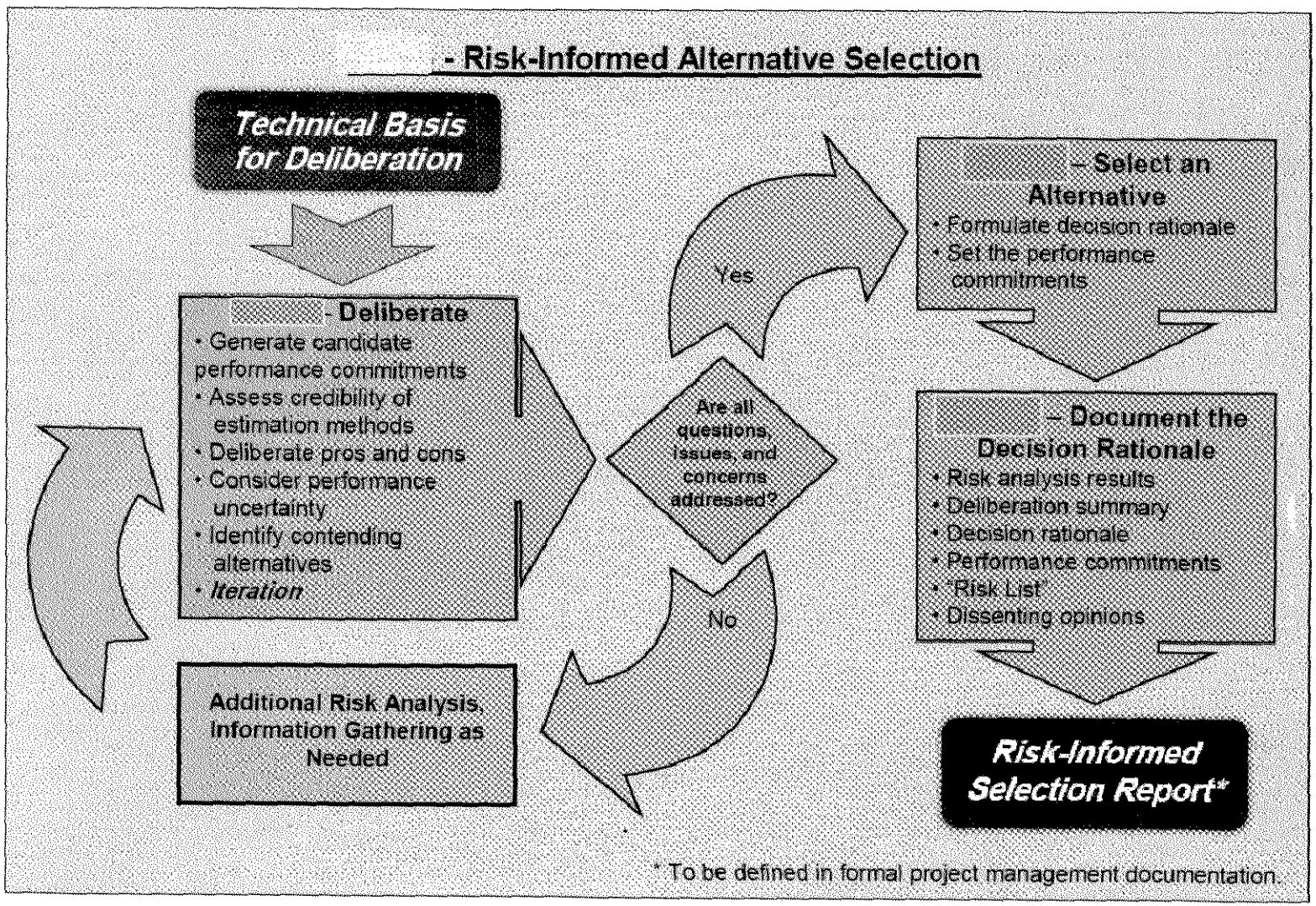
Pres
Cred

RIDM Process – Part 3

Summary of How the Concept of Performance Commitment Works

- The inputs to performance commitment development are
  - The performance measure pdfs for each decision alternative
  - An ordering of the performance measures
  - A risk tolerance for each performance measure, expressed as a percentile value
- The decision alternatives are compared by the decision maker in terms of candidate performance commitments that have the same failure probability across alternatives
  - Example ("Low" risk tolerance on previous slide):
    - Alternative B is best at the "low" risk tolerance setting (and Alternative A does not satisfy the imposed constraint)
    - Alternative A has the best reliability at the "low" setting
    - Alternative C has the best Cost & Schedule performance at the "low" setting
- The approach focuses DM attention on the level of program risk being assumed by selection of a given alternative at given commitment levels

Risk-informed Alternative Selection

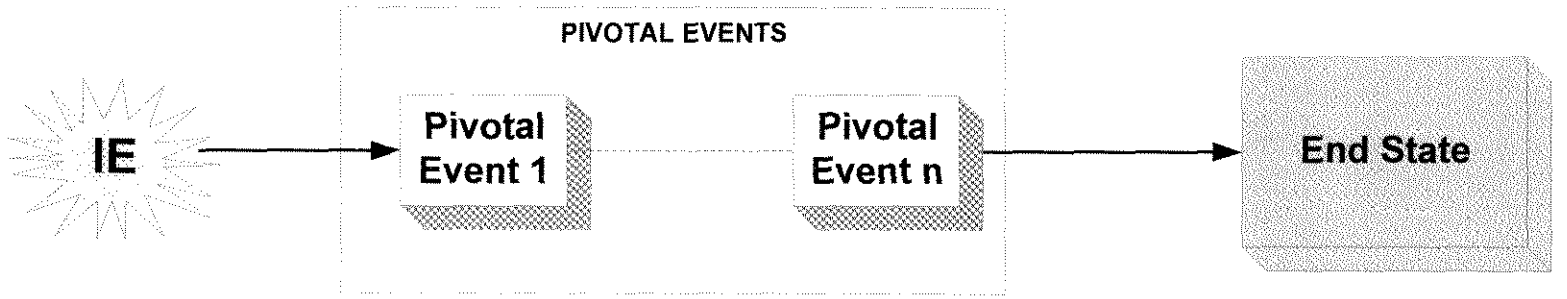


Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Probabilistic Risk Assessment Overview

Review of Some Key Concepts

The Concept of a Scenario



The perturbation

- Mitigative
- Aggravating

Consequence of interest to decision-maker

A risk scenario contains an IE and (usually) one or more pivotal events leading to an undesired end state.

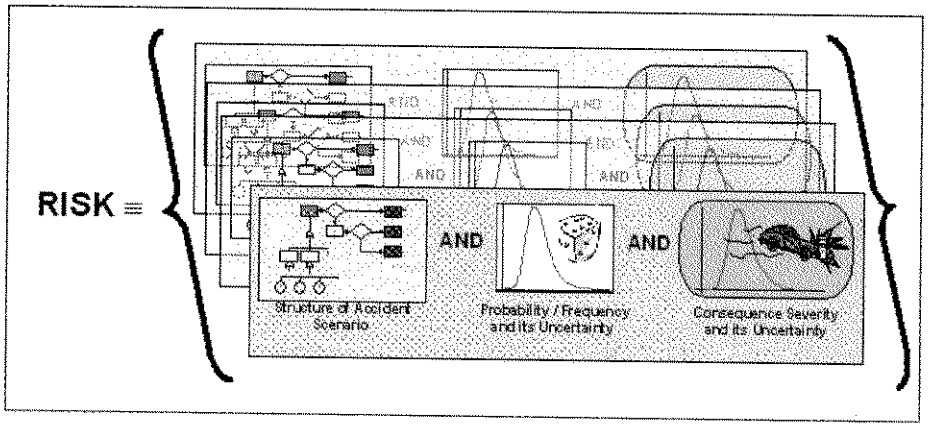
An Operational Definition for Risk

- **Risk is a set of triplets <S_i, P_i, C_i> that answer the questions :**
  - **What can go wrong? (scenarios, S_i)**
  - **How likely is it? (probabilities, P_i)**
  - **What are the consequences? (adverse effects, C_i)**

Kaplan & Garrick, Risk Analysis, 1981

$$R = RISK = \{\langle S_i, P_i, C_i \rangle\}$$

Scenario	Probability	Consequence
S_1	p_1	C_1
S_2	p_2	C_2
S_3	p_3	C_3
.	.	.
.	.	.
S_N	p_N	C_N



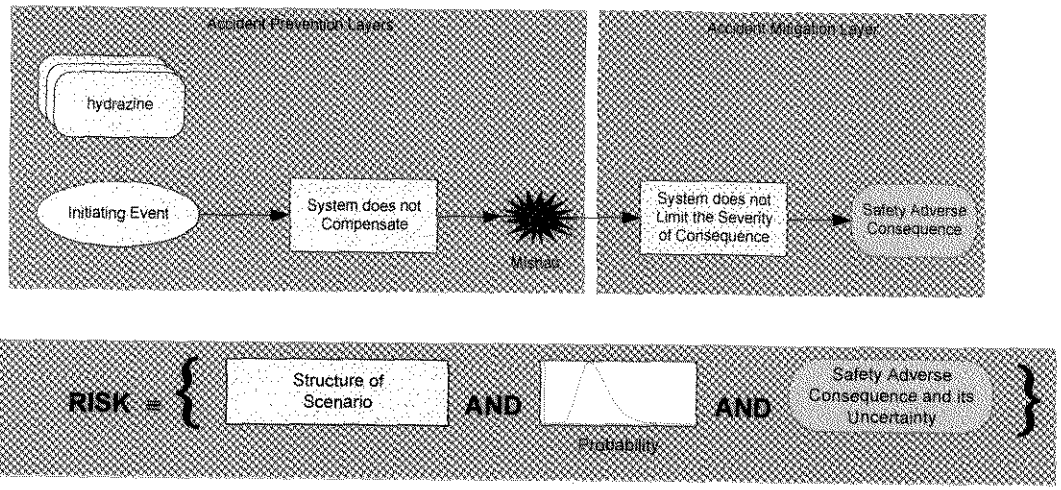
Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Hazard ≠ Risk

Examples of Hazard and Risk

- Hazard: **Hydrazine is *a hazard* because it can result or contribute to loss of spacecraft**

- Risk: **The risk scenario of <*Hydrazine leakage AND not detecting the leakage AND damaging flight critical avionics*> has probability of 1 in 10,000 to result in a loss of spacecraft**



Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

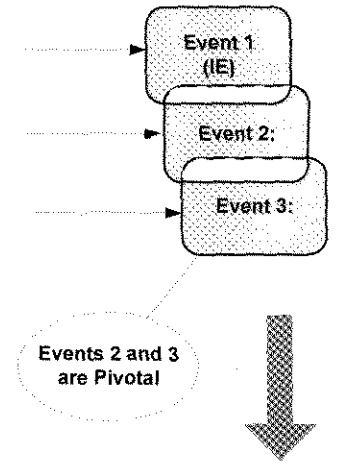
Pivotal Events

- In between IE and end states
  - Represent
    - successes or failures of system/crew responses to the IE
    - occurrence or non-occurrence of external conditions or phenomena
  - Mitigative: reduces the severity of a consequence
  - Aggravating: increases the severity of a consequence

Hydrazine leaks *and*

Leak is not isolated *and*

Damage to flight critical avionics



Loss of Spacecraft

Events:

- Building blocks of a scenario
- Declarative sentences used to characterize a scenario
- It is binary: Can only have two mutually-exclusive states (True or False)
- An event is a statement about a piece of equipment, a function, a condition, an outcome, etc.

Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

More on the Concept of Risk Scenarios

- A risk scenario is in effect a conditional statement.
- It is a logical expression that has the following structure:

Occurrence of certain event(s) → undesired end state

IF (IE ∩ Pivotal Event 1 ∩ Pivotal Event 2 ∩ ..), THEN undesired end state is reached

Where , ∩ for "and"

- A risk scenario is often characterized by a minimum set of events. In this case, the undesired end state can be ***prevented*** if
  - the IE does not occur <or>
  - one or more pivotal events do not occur

The "Event" Concept

- **Events: Building blocks of a scenario**
  - **declarative sentences used to characterize a scenario**
- **Each event is a statement about a piece of equipment, a function, a condition, an outcome, etc.**
  - **It is binary: Can only have two mutually-exclusive states (True or False).**
  - **Example:**

Leak is not detected (Failure Space)

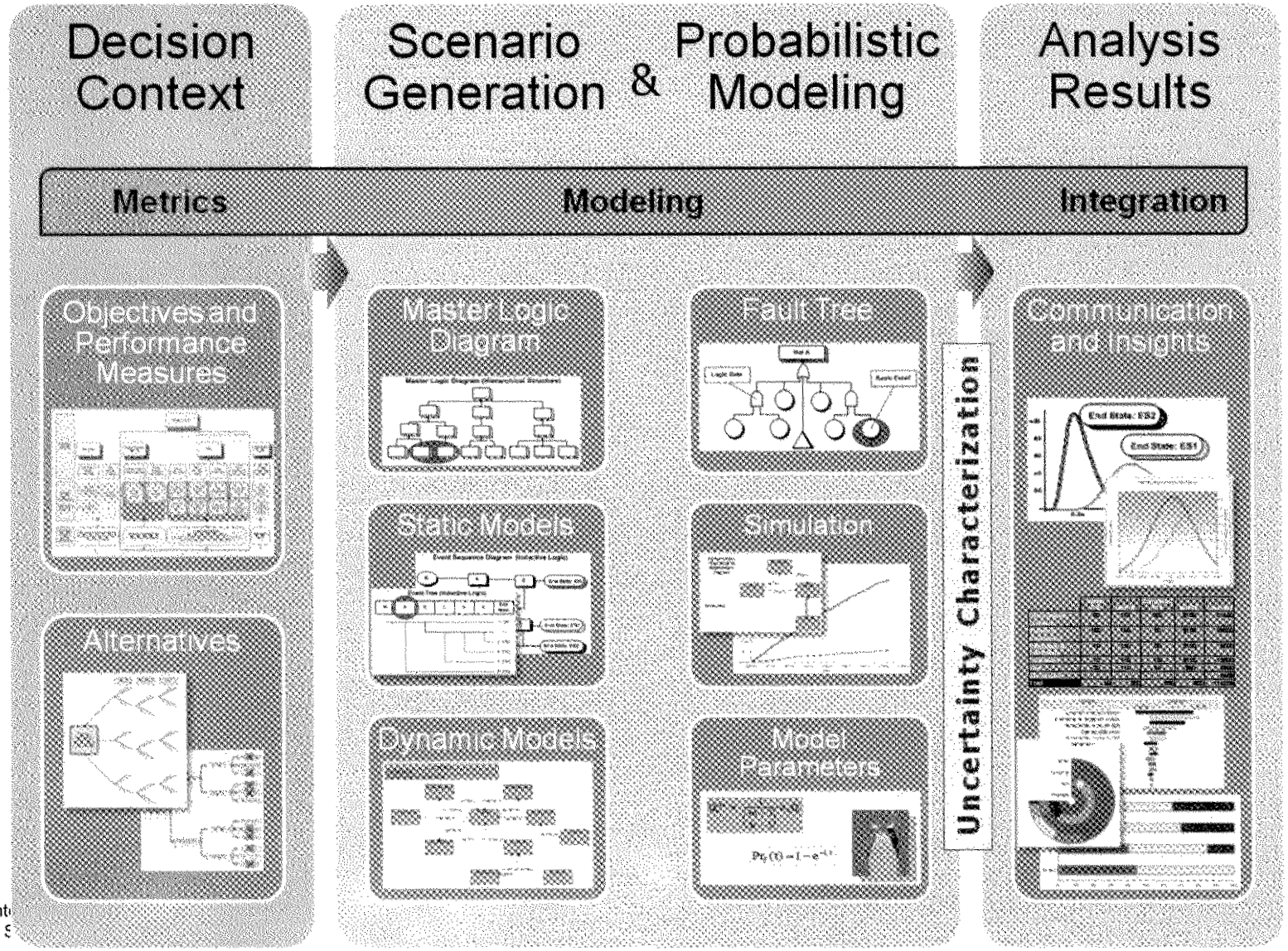
True	**Leak is not detected**
False	**Leak is detected**

Leak is detected (Success Space)

True	Leak is detected
False	Leak is not detected

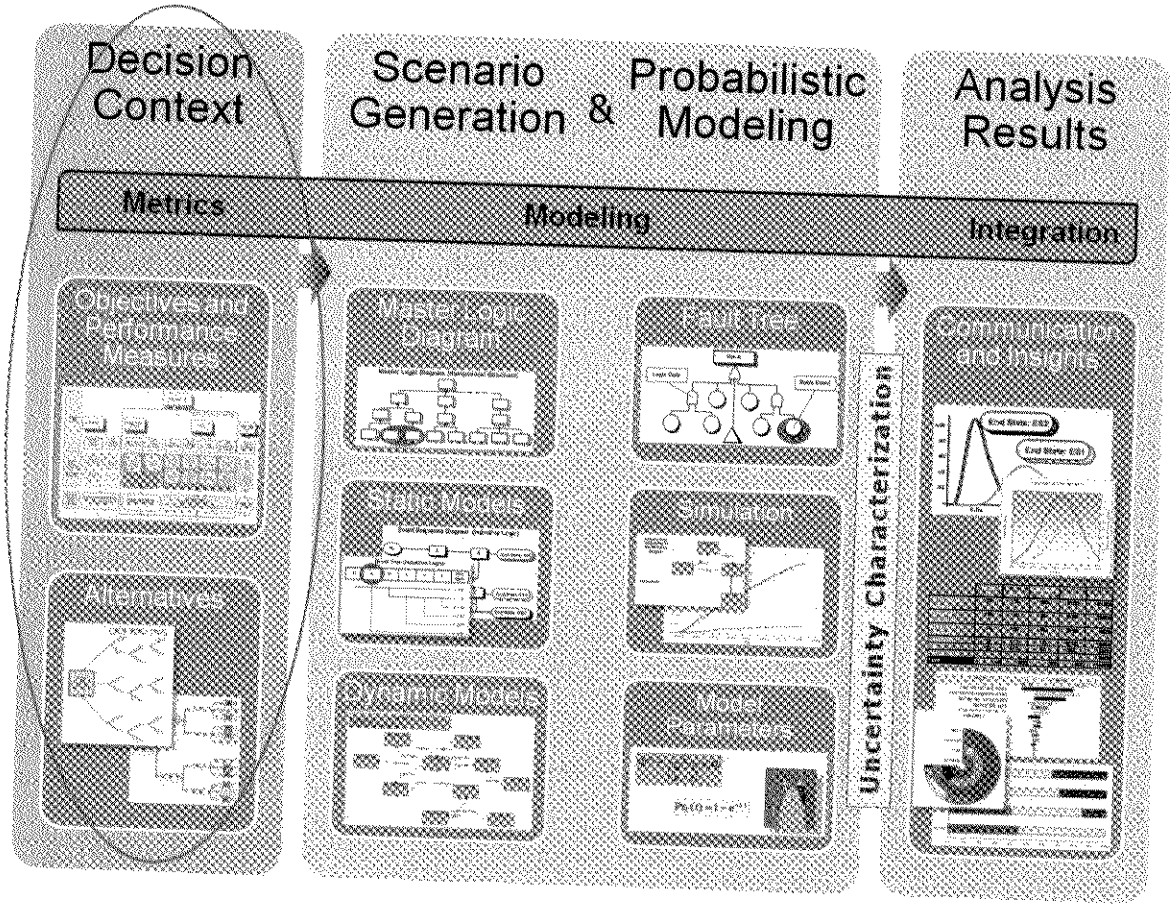
PRA Overview

PRA Methodology Synopsis



Present
Credit: S

Understanding the Decision Context

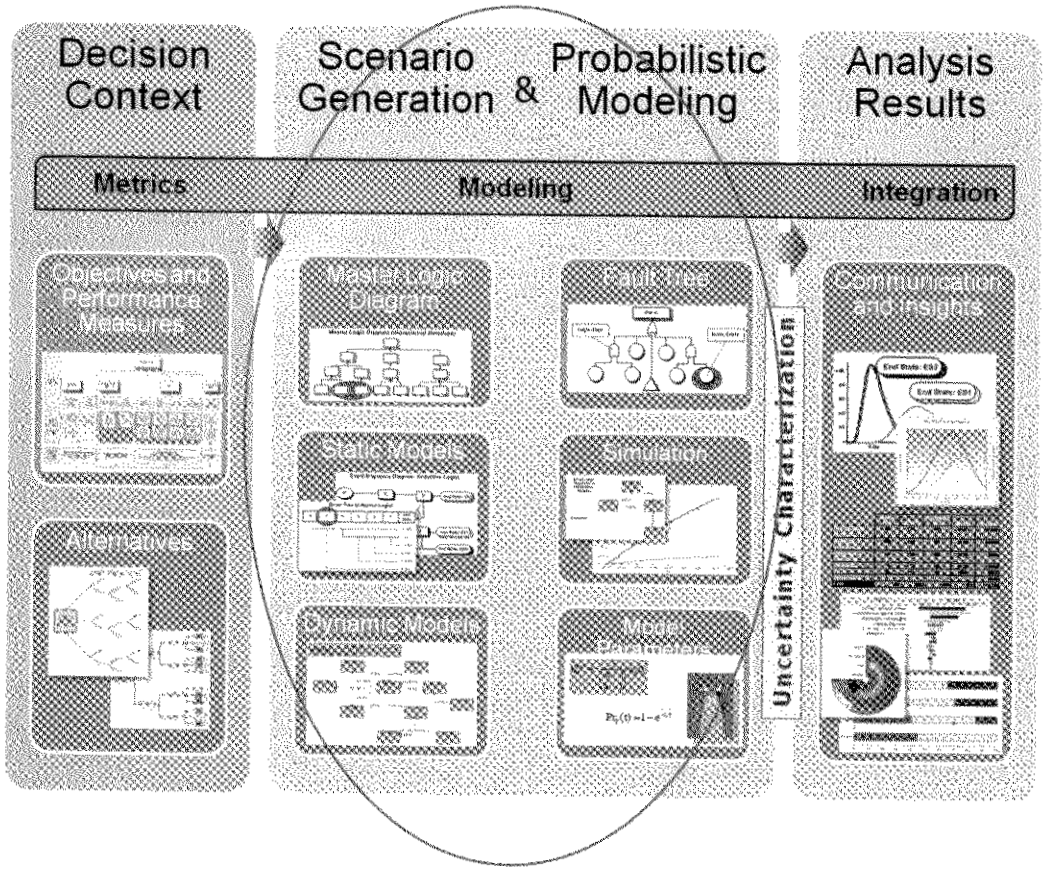


Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Decision Context

- If the PRA model is to be used to support decision making, then it should be structured to suit this purpose
- The performance measures (PMs) are defined according to decisions being supported
- Identification of PMs is the starting point of the PRA process
  - They should serve the evaluation of decision options
  - Ultimately they should be quantified
- Examples of PMs:
  - P(loss of life or injury / illness to crew)
  - P(damage to, or loss of, equipment or property)
  - P(evacuation)
  - P(failure of mission)
  - P(damage to environment)

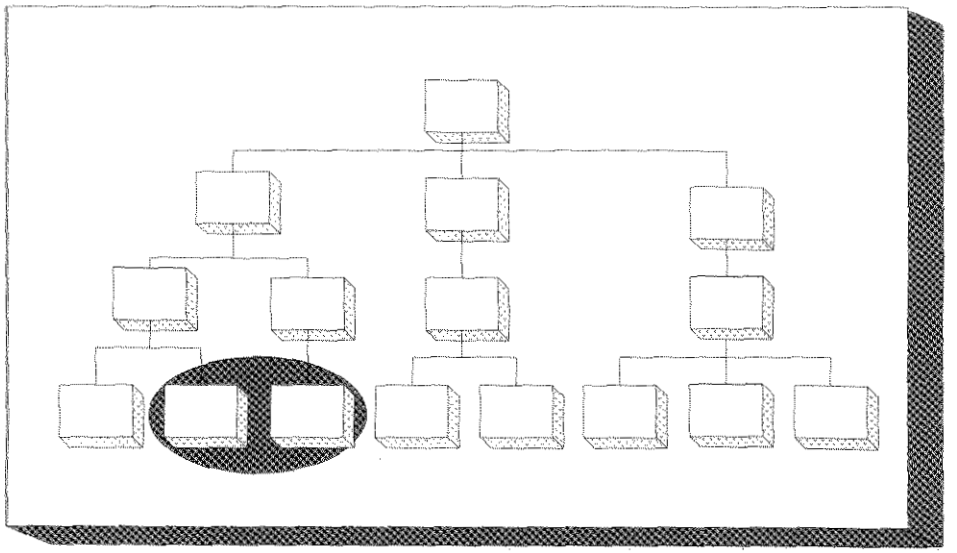
Scenario Structuring



System Familiarization

- Development of a comprehensive scenario set for a complex facility or mission is a team effort because of
  - the volume of work and
  - diversity of technical discipline involved
- PRA requires detailed knowledge of responses to perturbations
- PRA analysts require an in-depth knowledge of the system and how it operates.
  - knowledge of system dependencies;
  - knowledge of system operability states
- Knowledge of "How it Fails" is derived from "How it Works"
- PRA team should include system experts

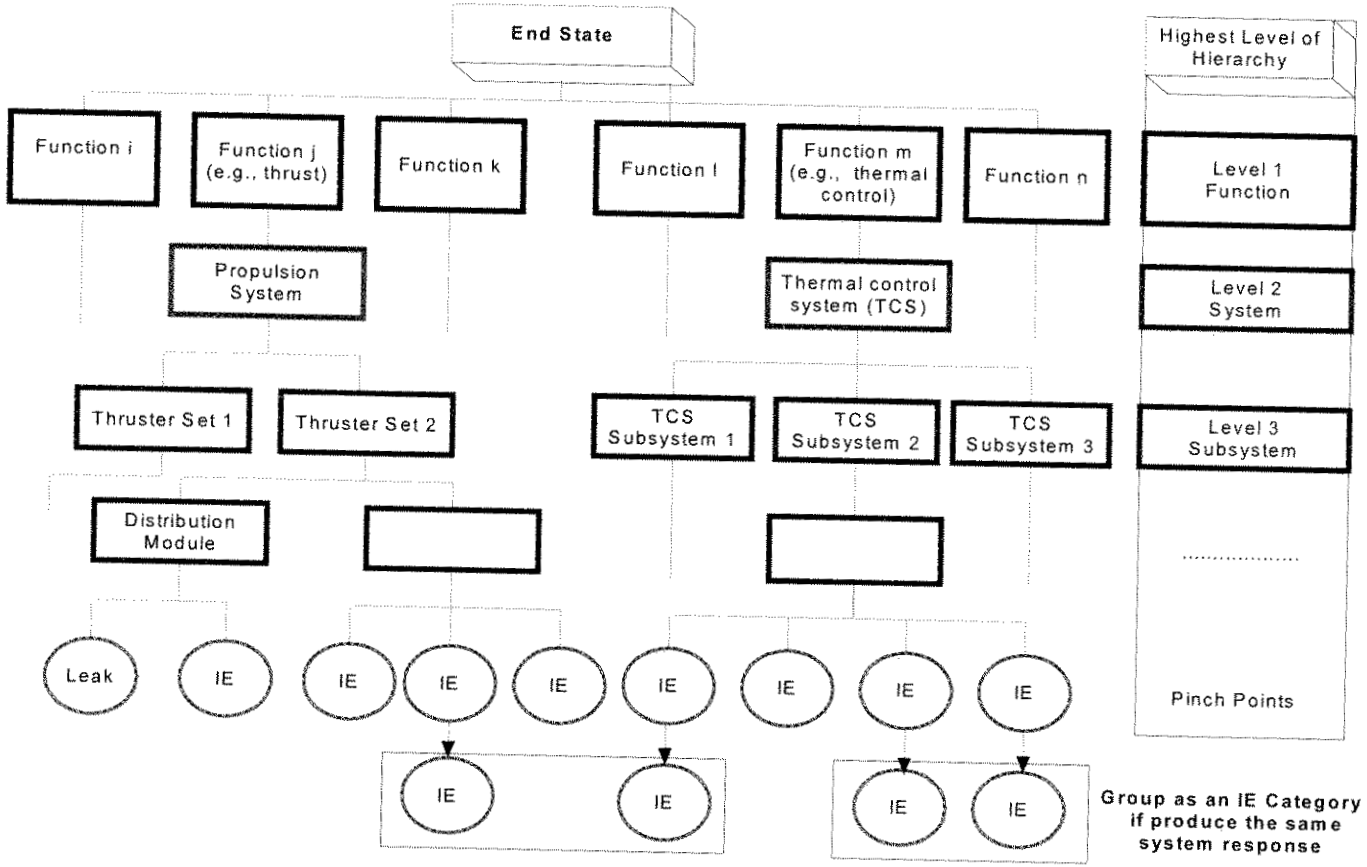
Initiating Events (IEs)



Master Logic Diagram (MLD)

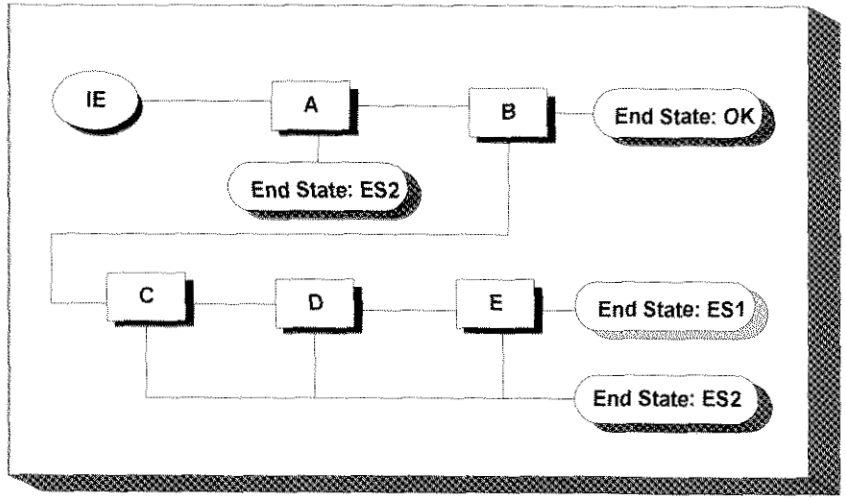
- Hierarchical (Top-Down) method for obtaining initiating event *groups* (CLASS OF THINGS THAT CAN GO WRONG?)
- The highest level of hierarchy is the end state of interest
- Intermediate levels identify systems and subsystems (e.g., thruster module fails)
- Lower levels identify component assemblies and initiating event categories (e.g., filter clogs or propellant leaks)
- Master Logic Diagram is completed when further breakdown produces same system responses as higher level
- An important consideration in the development of a useful MLD is knowing when to stop at a reasonable level
- The "pinch point" occurs when every level below the stopping level has the same consequence as the level above it

Initiating Events: Master Logic Diagram (MLD)



Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

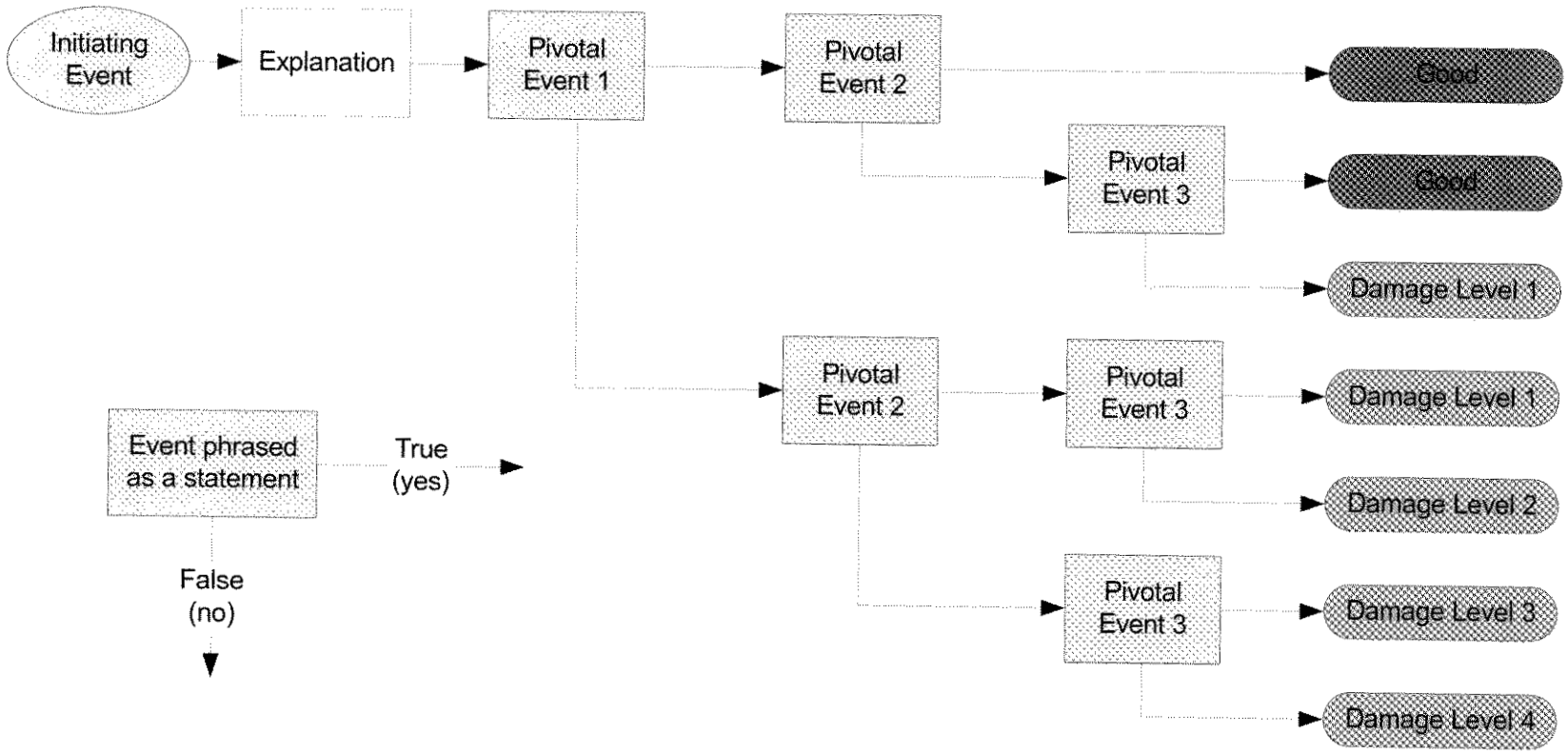
Event Sequence Diagram (ESD)



Structuring Scenarios

- ESD is useful for identifying accident scenarios
- The method uses forward logic
- An ESD is developed for each initiating event category in the Master Logic Diagram
- Most engineers find ESDs intuitive and easy to understand:
  - Used for communication between PRA analysts and system engineers
- Events may be ordered to reflect dependence:
  - Later events depend on earlier events
- Similarities in system response indicate that different initiating events can be combined
- Scenario modeling is not typically accomplished in a single pass

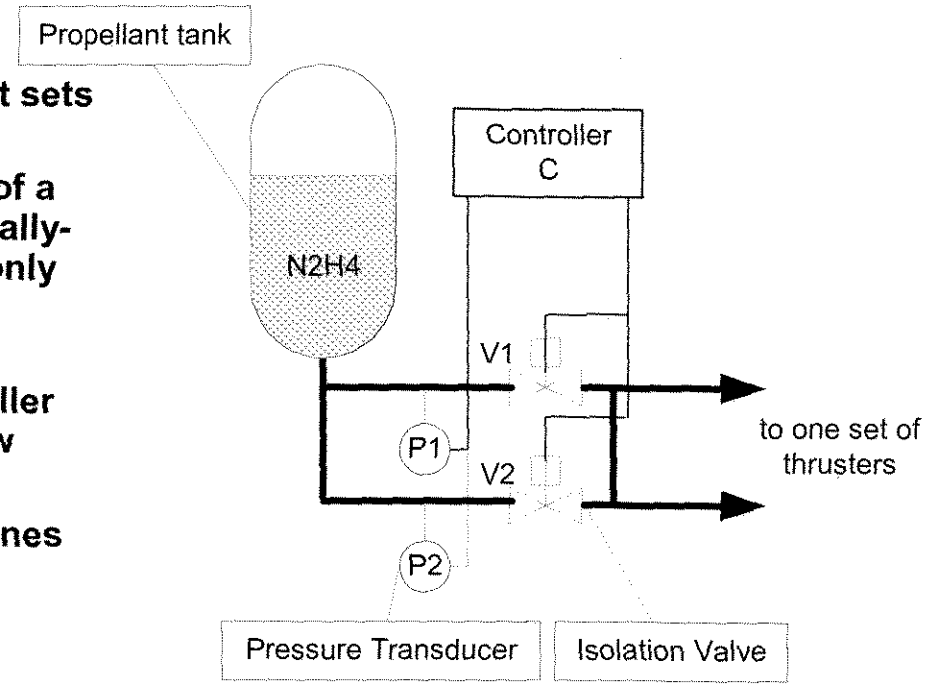
A Typical ESD



Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

A Simple Example

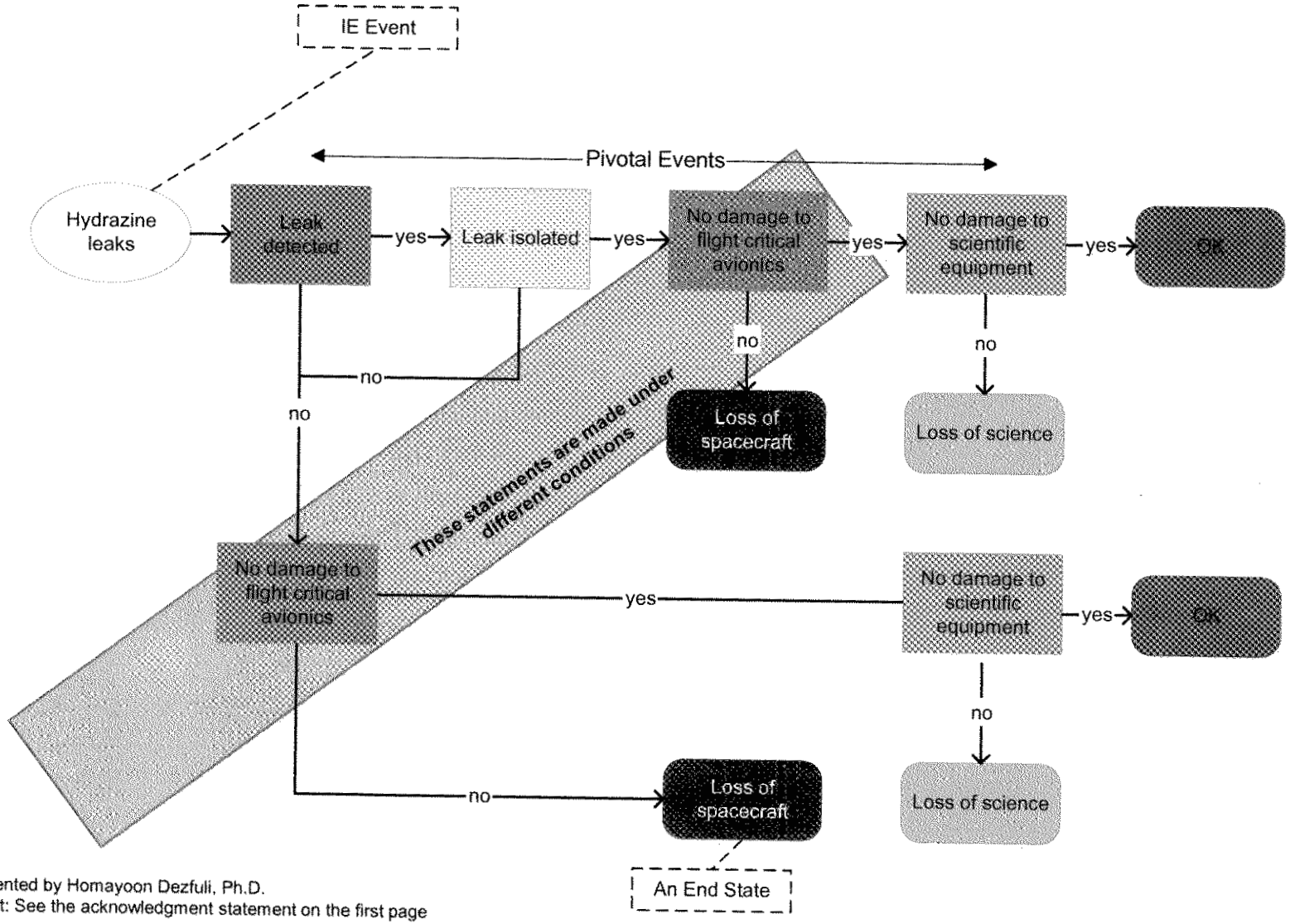
- The spacecraft is designed with two redundant sets of thrusters (independent of each other)
- Each propellant distribution module consists of a hydrazine tank, filters, distribution lines, normally-open isolation valves, sensors, heaters, etc. (only components that affect mitigation of leaks are shown)
- When thruster operation is needed, the controller opens the solenoid valves (not shown) to allow hydrazine to flow
- The controller monitors the pressure of feed-lines via pressure transducers (P1 and P2). It is designed to differentiate between the normal thruster operation and a leak
- In the event of a leak, isolation valves (V1 and V2) should both close
- Successful termination of the leak leads to the loss of one but not both, thruster sets
- Failure to terminate the leak can cause damage to the flight critical avionics and/or damage to scientific equipment:
  - Hydrazine acts as a wire stripper and is corrosive



Simplified Schematic of Propellant Distribution Module

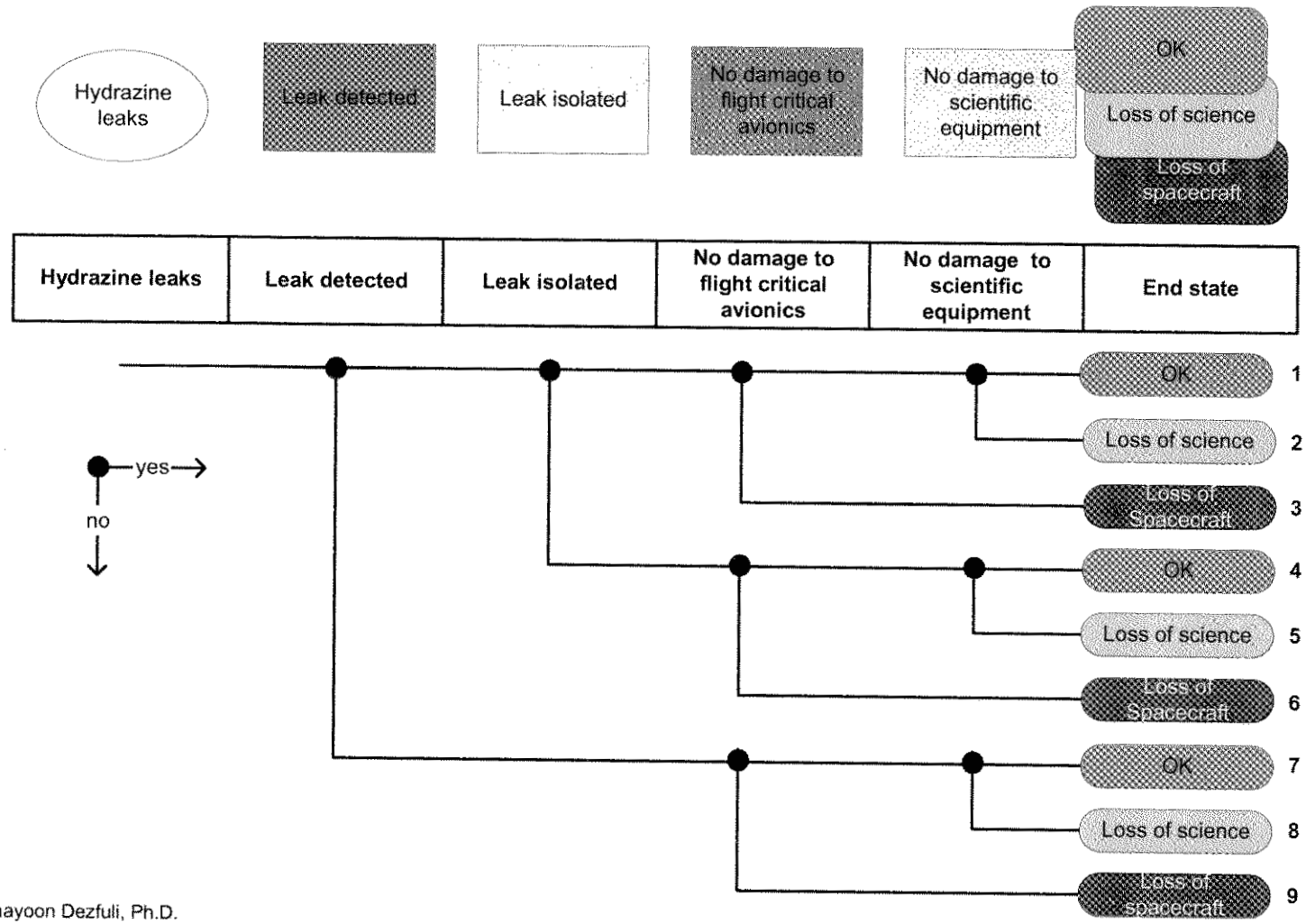
Space mission type: scientific
PMs of interest
Probability (loss of spacecraft)
Probability (loss of science data)
Propose design modification, if needed

ESD for Propellant Leak



Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Constructing Event Trees for Propellant Leak



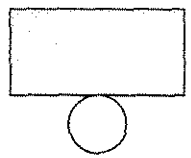
Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Fault Tree Modeling of Pivotal Events

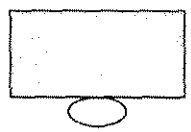
- Most popular way to "map" component level failure information to "system level" failure information
- It is a "top-down" analysis
- Used to analyze initiating or pivotal events in terms of more detailed, causal events
- Breakdown continues until either
  - data are available for quantification, or
  - scope of work dictated level of disaggregation.
- Typically, the lowest level (called "basic event" level) is the largest level of assembly for which data are available

Fault Tree Symbols (Basic Events)

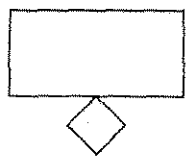
PRIMARY EVENT SYMBOLS



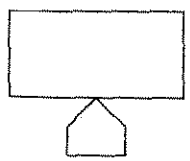
BASIC EVENT – A basic initiating fault requiring no further development



CONDITIONING EVENT – Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY, AND and INHIBIT gates).



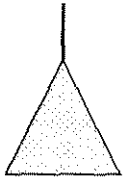
UNDEVELOPED EVENT – An event which is not further developed either because it is of insufficient consequence or because information is unavailable.



HOUSE EVENT – An event which is normally expected to occur.

Fault Tree Symbols (Transfers)

TRANSFER SYMBOLS

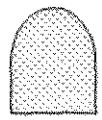


TRANSFER IN – Indicates that the next tree is developed further at the occurrence of the corresponding **TRANSFER OUT** (e.g. on another page)

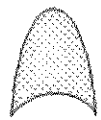
TRANSFER OUT – Indicates that this portion of the tree must be attached at the corresponding **TRANSFER IN**

Fault Tree Symbols (Gates)

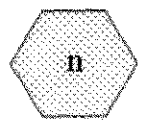
GATE SYMBOLS



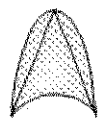
AND – Output fault occurs if all of the input faults occur.



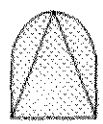
OR – Output fault occurs if at least one of the input faults occur.



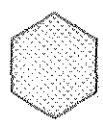
COMBINATION – Output fault occurs if n of the input faults occur.



EXCLUSIVE OR – Output fault occurs if exactly one of the input faults occurs.

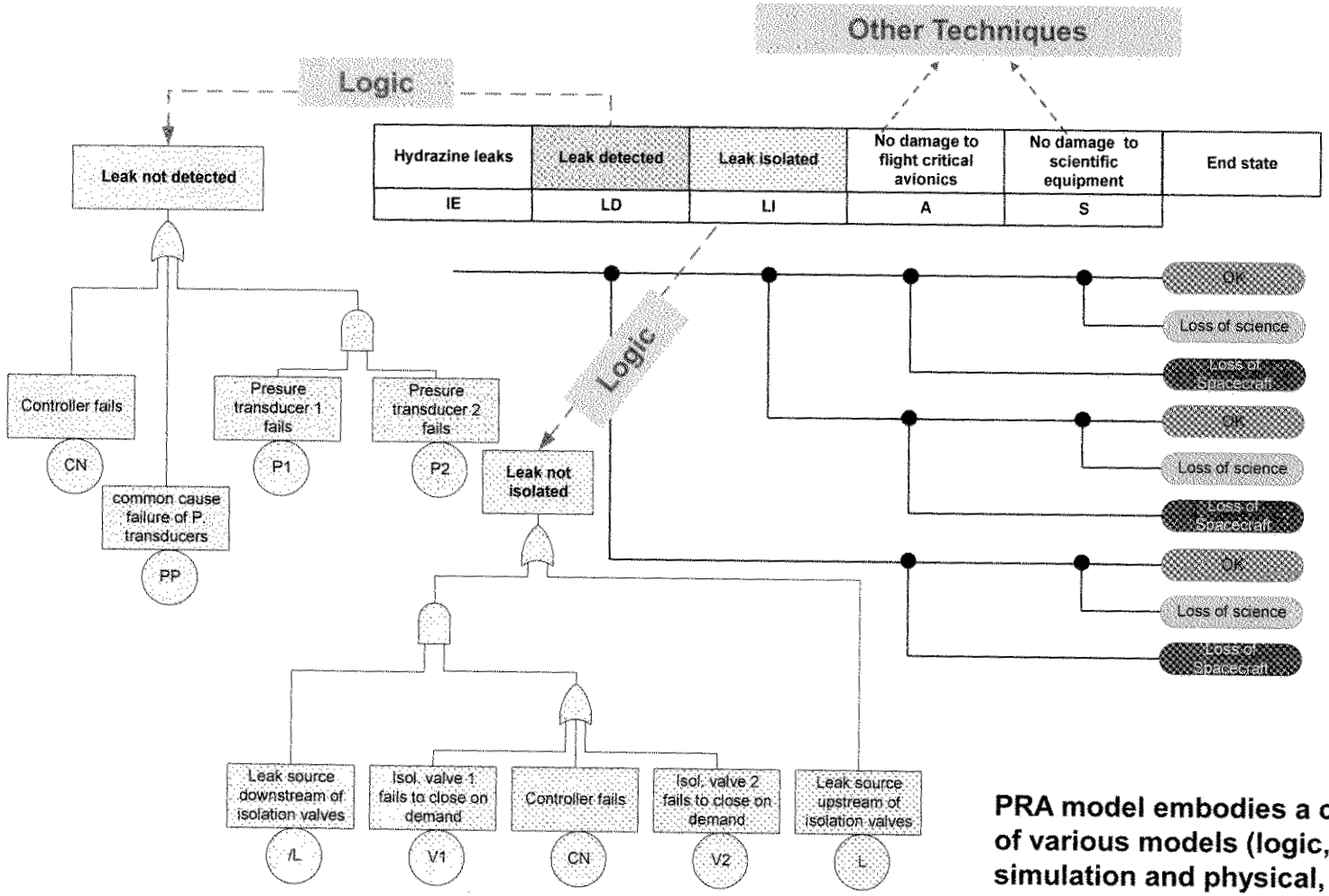


PRIORITY AND – Output fault occurs if all of the input faults occur in a specific sequence. The sequence is represented by a CONDITIONING EVENT drawn to the right of the gate.



INHIBIT – Output fault occurs if the (single) input fault occurs in the presence of an enabling condition. The enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate.

Fault Tree Modeling of Pivotal Events (Cont.)



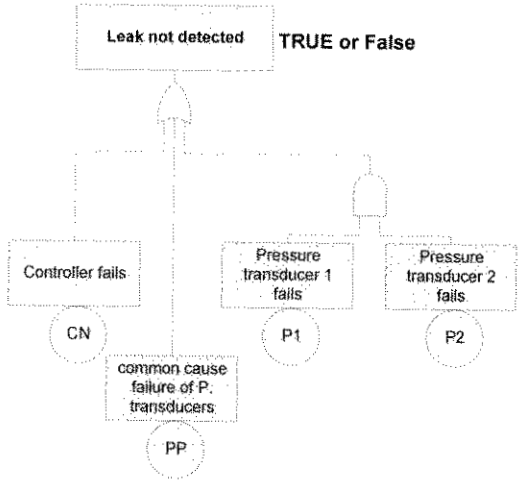
PRA model embodies a collection of various models (logic, reliability, simulation and physical, etc.) in an integrated structure

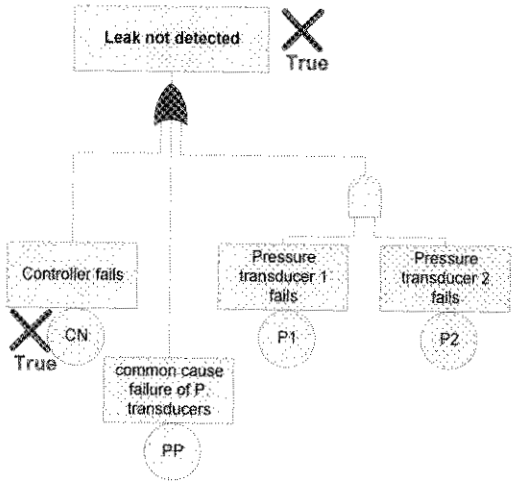
Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

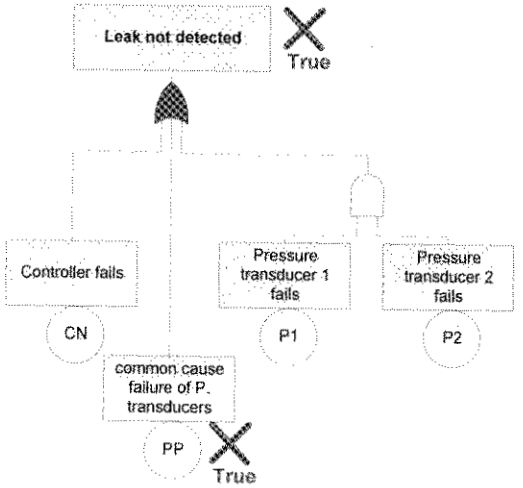
The Concept of Cut Sets

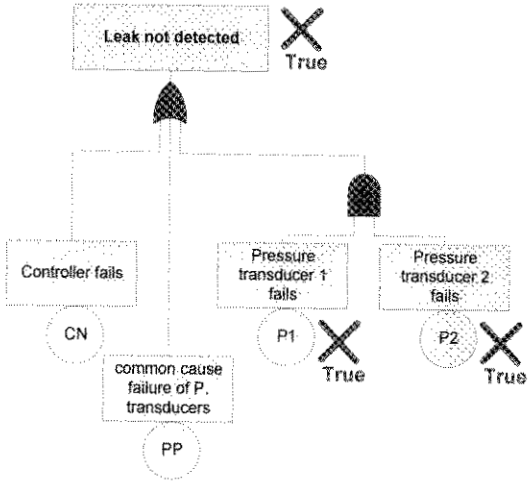
- The primary reason for logic-based decomposition of IEs or pivotal events into more detailed causal events (primary events) is the identification of cut sets
- Cut set: A set of primary events whose simultaneous occurrence guarantees the occurrence of the top event (pivotal event)
- Minimal cut set: A cut set containing the minimum subset of primary elements whose simultaneous occurrence guarantees the occurrence of the top event
  - If one were to remove one of the events in a minimal cut set, the top event would not occur

Min Cut Sets for Pivotal Event (Leak not isolated)









Let "T" symbolize "Leak not detected"

The minimal cut sets for event T

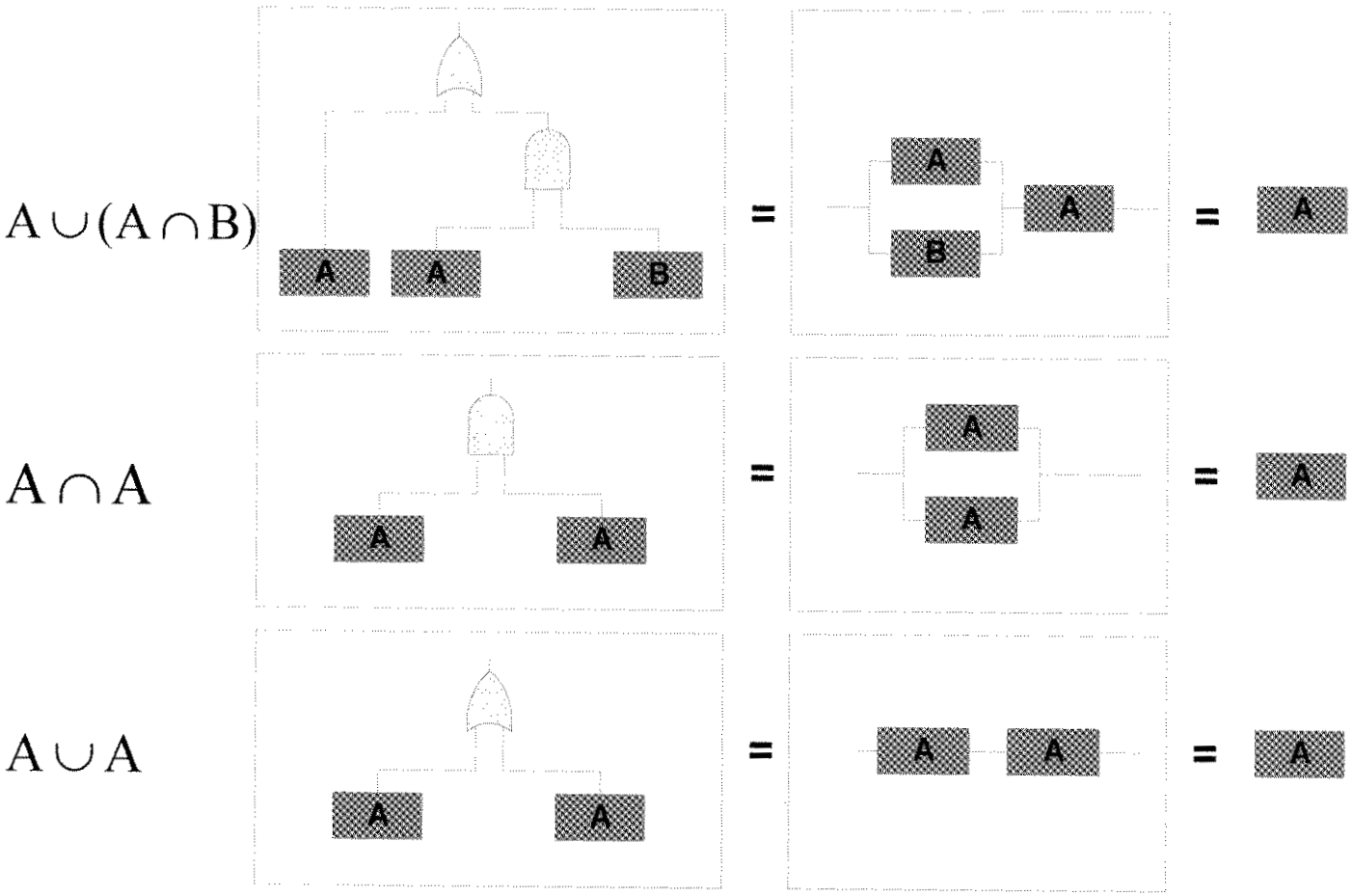
$T = CN \cup PP \cup (P1 \cap P2)$

How to read it:

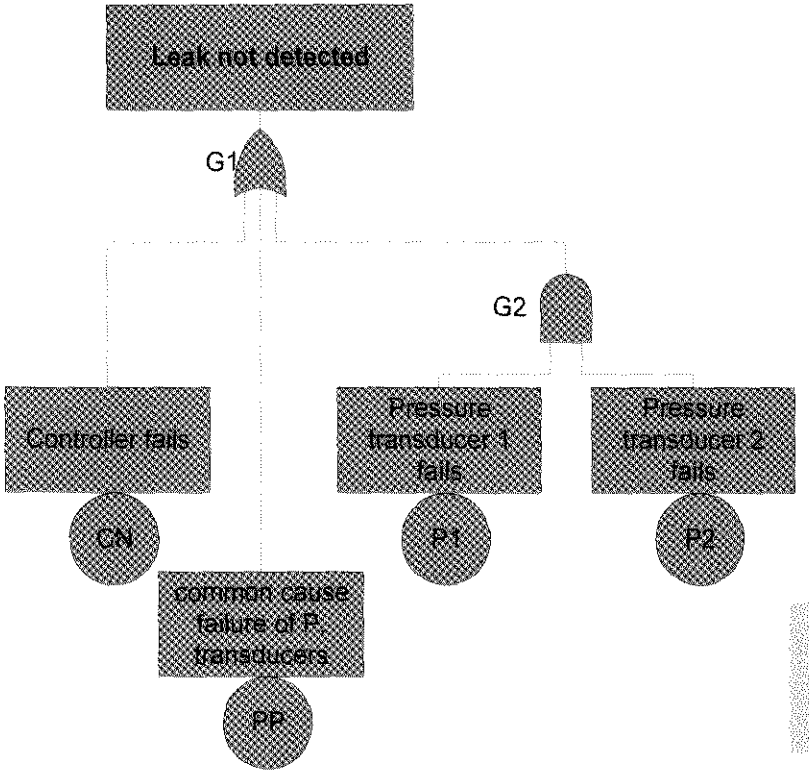
T occurs IF { CN occurs OR PP occurs OR P1 and P2 both occur}

Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Examples of Rules of Boolean Algebra



Minimal Cut Sets for Pivotal Event (Leak not Detected)



$G2 = P1 \cap P2$

$G1 = CN \cup PP \cup G2$

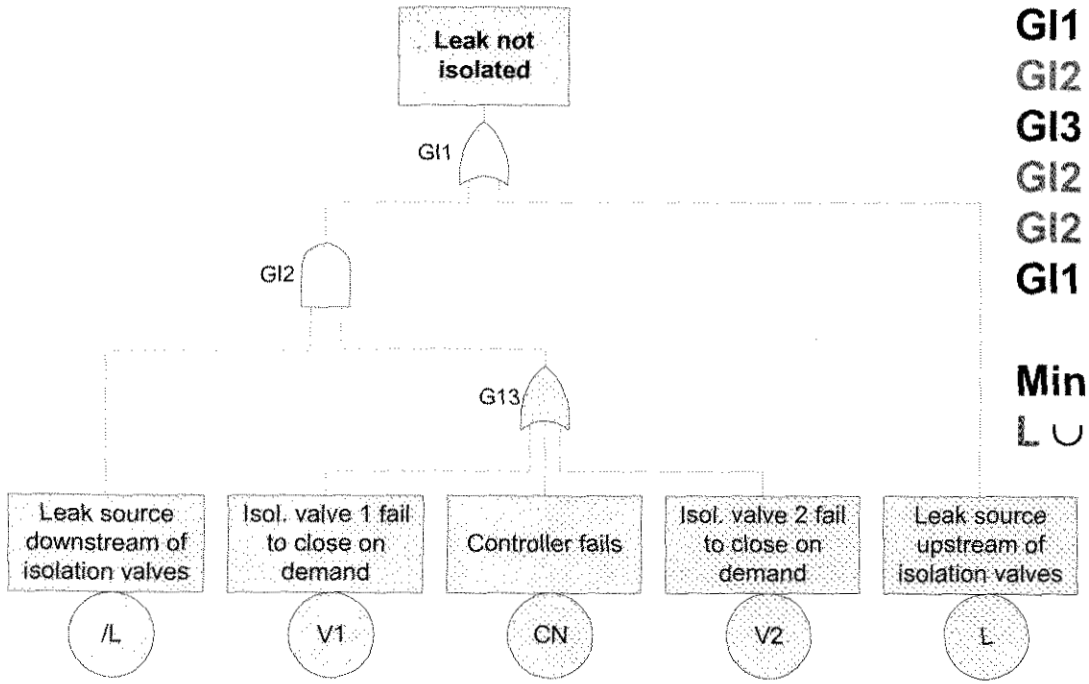
$G1 = CN \cup PP \cup (P1 \cap P2)$

Minimal cut sets

$CN \cup PP \cup (P1 \cap P2)$

Minimal cut set: A minimum set of basic elements whose simultaneous occurrence guarantees the occurrence of the top event

Minimal Cut Sets for Pivotal Event (Leak not isolated)

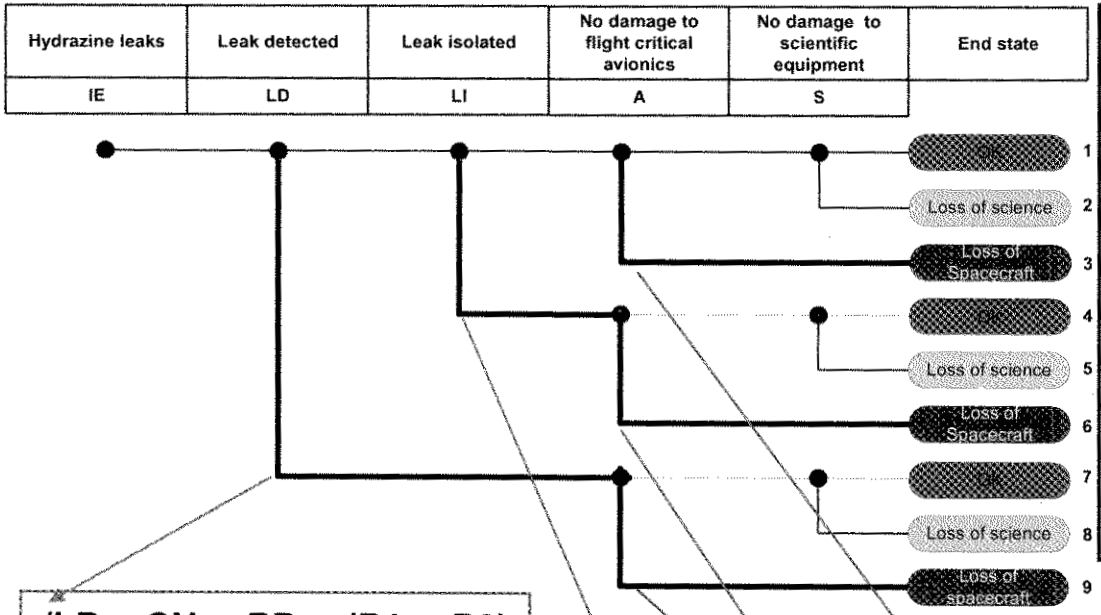


$GI1 = L \cup GI2$
$GI2 = /L \cap GI3$
$GI3 = V1 \cup V2 \cup CN$
$GI2 = /L \cap (V1 \cup V2 \cup CN)$
$GI2 = (/L \cap V1) \cup (/L \cap V2) \cup (/L \cap CN)$
$GI1 = L \cup (/L \cap V1) \cup (/L \cap V2) \cup (/L \cap CN)$

Minimal cut sets

$L \cup (/L \cap V1) \cup (/L \cap V2) \cup (/L \cap CN)$

One-to-Many Mapping of Scenarios 3, 6, and 9



Risk Scenario	ONE-TO-MANY MAPPING	
	As defined in Event Tree	Mapping to basic events
3	IE∩LD∩LI∩/A1	IE∩LD∩LI∩/A1
6	IE∩LD∩/LI∩/A2	IE∩LD∩L∩/A2 IE∩LD∩/L∩V1∩/A2 IE∩LD∩/L∩V2∩/A2 IE∩LD∩/L∩CN∩/A2
9	IE∩/LD∩/A2	IE∩CN∩/A2 IE∩PP∩/A2 IE∩P1∩P2∩/A2

/LD = CN ∪ PP ∪ (P1 ∩ P2)

/A1

/A2

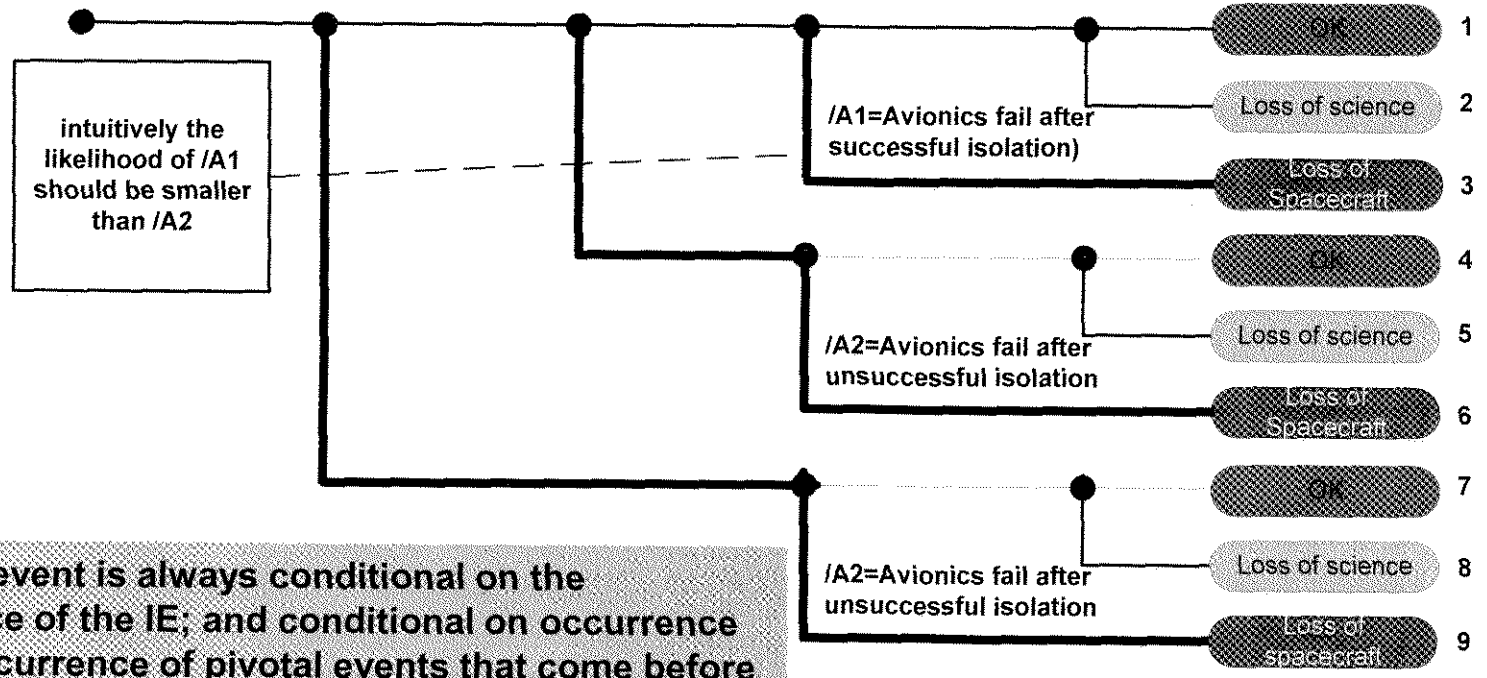
Can this scenario occur?

/LI = L ∪ (/L ∩ V1) ∪ (/L ∩ V2) ∪ (/L ∩ CN)

Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Conditional Events

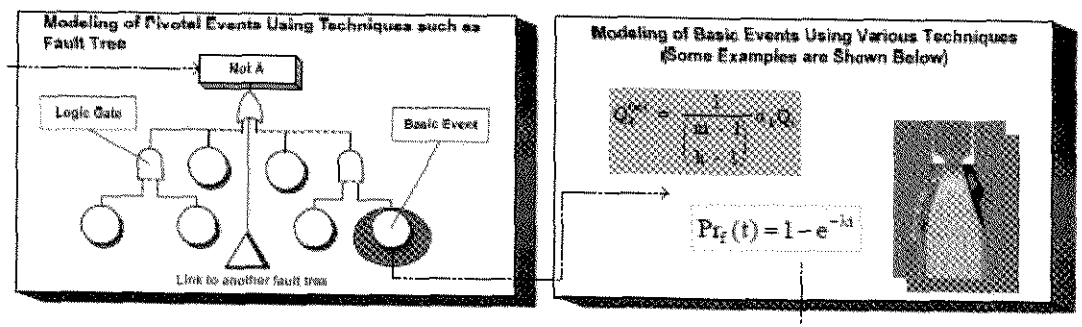
Hydrazine leaks	Leak detected	Leak isolated	No damage to flight critical avionics	No damage to scientific equipment	End state
IE	LD	LI	A	S	



- **A pivotal event is always conditional on the occurrence of the IE; and conditional on occurrence or non occurrence of pivotal events that come before that**
- **Characterization of pivotal events as conditional events is essential in order to properly quantify them**

Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Probabilistic Modeling



Type of Events that Appear in the Structure of Scenarios

- Hardware failure: failure mode(s) of hardware components
  - Example: isolation valve fails to close on demand
- Software failure
  - Example: controller program fails to generate isolation signal due to a software error
- Phenomenological: a sequence of physical, chemical or biological events
  - Example: Propellant Leak damages critical wire harnesses for avionics
- Human error: omission or commission errors
  - Example: Crew fails to isolate the leak after automatic isolation fails
- Common cause failure (CCF): Failure of multiple components due to common physical environment or human interaction
  - Example : common cause failure of both pressure transducers

Data Development

- Events appear in the structure of scenarios are treated as uncertain quantities for which we need probability estimates. Sources of data:
  - Hardware
    - Historical data on a similar piece of equipment
    - General engineering knowledge about the equipment or an expert's experience with the equipment
  - Phenomenological
    - Experimental and simulation models
    - Expert judgment
  - Human error
    - Simulator data
    - Actuarial data
    - Expert judgement
  - Common cause failure
    - Parametric models (e.g., beta factor)

Use of Reliability Models to obtain Probability Estimates (an example)

- **The simplest and widely-used model based on the assumption of exponential time-to-failure**

- **Probability of failure:**

$$Pr_f(t) = 1 - e^{-\lambda t}$$

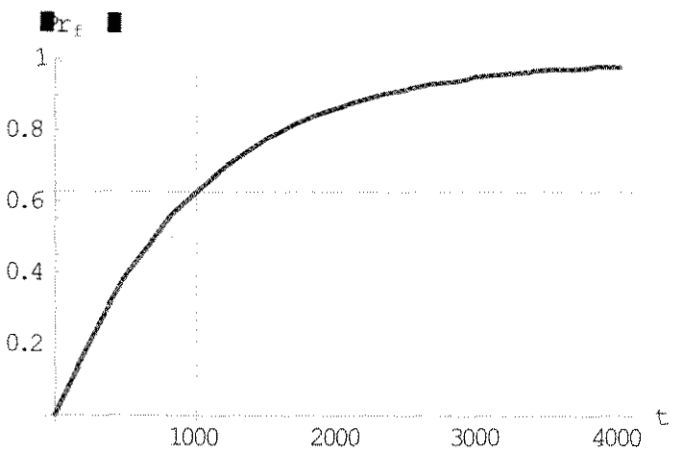
Example: assume λ = 0.001 per hour

the probability that the device will fail before t=1000 hours is

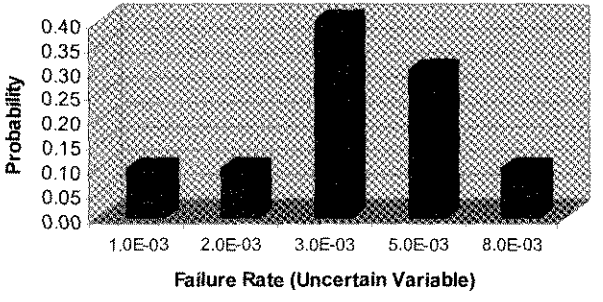
1- exp(-1)=0.632

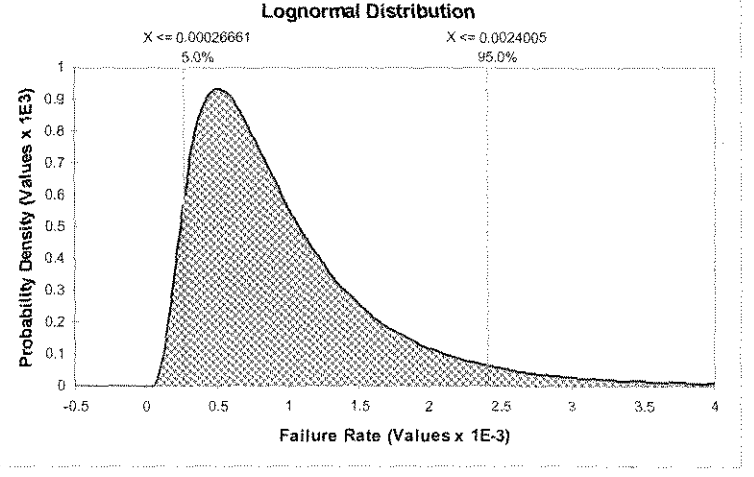
the probability that the device works for at least 1000 hours is

1- 0.632=0.368



Uncertainty Expressed as Probability Distribution





Typical uncertainties are associated with

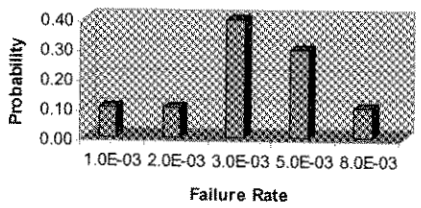
- **Numerical values of the parameters used in the model**
- **Inherent variability of stochastic processes**

Bayes' Theorem

- The types of information available for the frequency of basic events include:
  - prior knowledge such as general engineering knowledge and the historical information from similar events,
  - the observed data for the event of interest in the system under study
- The Bayesian approach provides a formal mechanism for combing all available information, such as engineering and qualification test data, filed experience, expert judgment, and data from similar systems

Bayes' Theorem (cont.)

$\pi_0(\lambda)$



$$L(E|\lambda) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

Model: Poisson
Evidence: K failures in t hours of operation
K=2; t=1000 hours

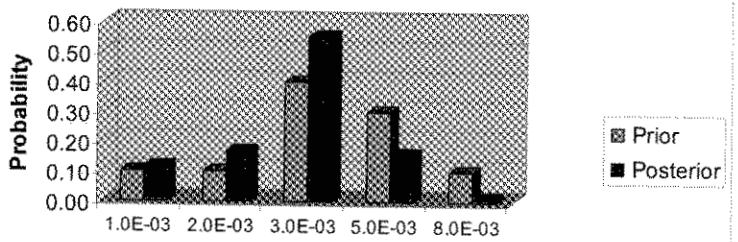
Our prior knowledge about the failure rate

Our model and observed data (evidence E)

$$\pi_1(\lambda|E) = \frac{\pi_0(\lambda) \bullet L(E|\lambda)}{k}$$

Use Bayes' Theorem to combine our prior knowledge and our evidence

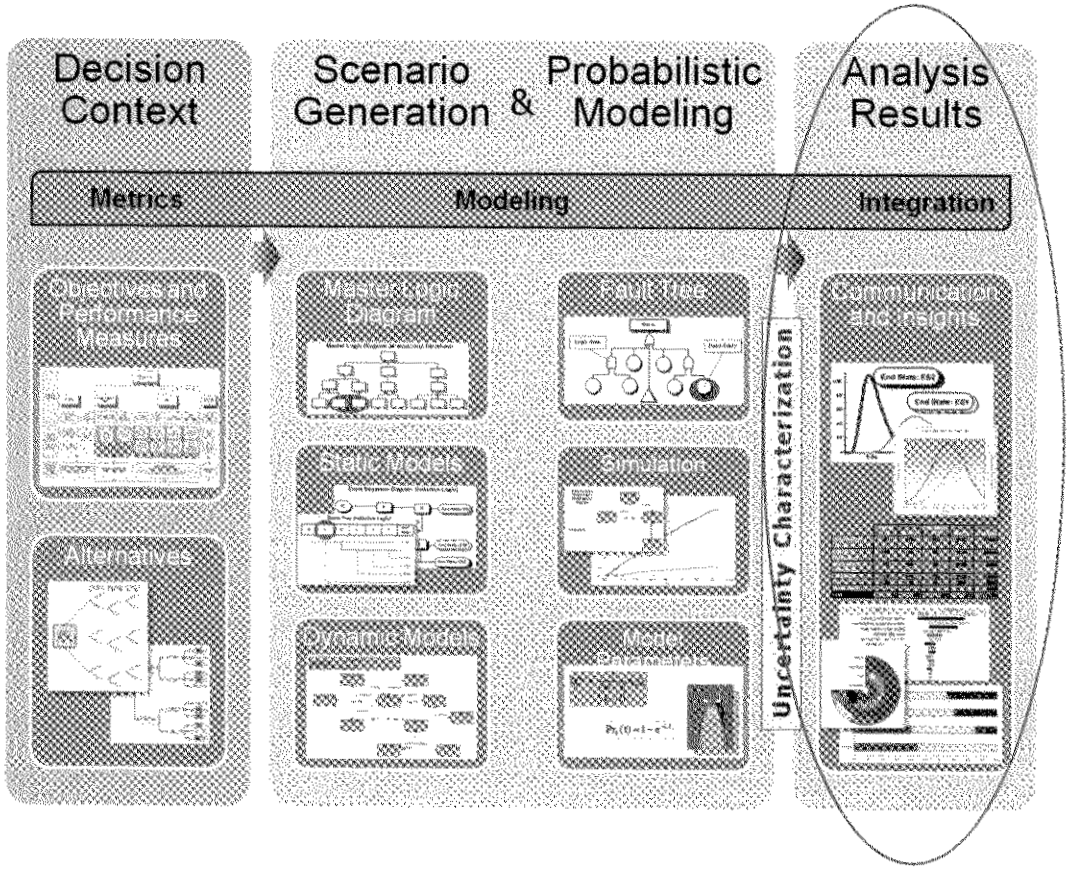
Comparison of Prior and Posterior



Probability Values Assigned to Basic Events of Example Problem

Event Name	probability	Comment
CN	1.00E-04	
P1	1.00E-03	
P2	1.00E-03	
PP	1.00E-04	
L	1.00E-01	L and /L should add up to unity
V1	1.00E-03	
V2	1.00E-03	
/L	9.00E-01	
/A1	1.00E-05	Conditional Pr. for the first branch of A
/A2	1.00E-01	Conditional Pr. for the 2nd & 3rd branch A
IE	1.00E-02	Frequency per mission

Analysis Results for the Example Problem



Frequency of Leak Initiated Scenarios that Lead to Loss of Vehicle

Scenario	Description of Scenario	Cut Set	Symbol	Meaning	Probability	Total
3	Hydrazine Leak, Isolated Promptly but Avionics Fail Anyway	1	IE	Leak	1.0E-2	1.0E-7
			/A1	Avionics fail even after successful isolation	1.0E-5	
9	Hydrazine Leak, Detection Failure Leading to Isolation Failure, Avionics Failure	2	IE	Leak	1.0E-2	1.0E-7
			PP	Common cause failure of pressure transducers	1.0E-4	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		3	IE	Leak	1.0E-2	1.0E-7
			CN	Controller fails	1.0E-4	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		4	IE	Leak	1.0E-2	1.0E-9
			P1	Pressure transducer 1 fails	1.0E-3	
			P2	Pressure transducer 2 fails	1.0E-3	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
6	Hydrazine Leak, Detection Succeeded but Isolation Fails, Avionics Failure	5	IE	Leak	1.0E-2	1.0E-4
			L	Leak occurs upstream of isolation valves	1.0E-1	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		6	IE	Leak	1.0E-2	9.0E-7
			/L	Leak occurs downstream of isolation valves	9.0E-1	
			V2	Isolation valve V2 fails to close	1.0E-3	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		7	IE	Leak	1.0E-2	9.0E-7
			/L	Leak occurs downstream of isolation valves	9.0E-1	
			V1	Isolation valve V1 fails to close	1.0E-3	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
					Total	1.02E-4

Dominant Risk Scenario

Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Characterizing Frequency of Events as Uncertain Quantities

- **We are uncertain about the value of parameter(s) used to model occurrence probability of each event in the right**
  - **Example: We are uncertain about the value of the failure rate λ that we assumed in the exponential failure model of Event "CN"**

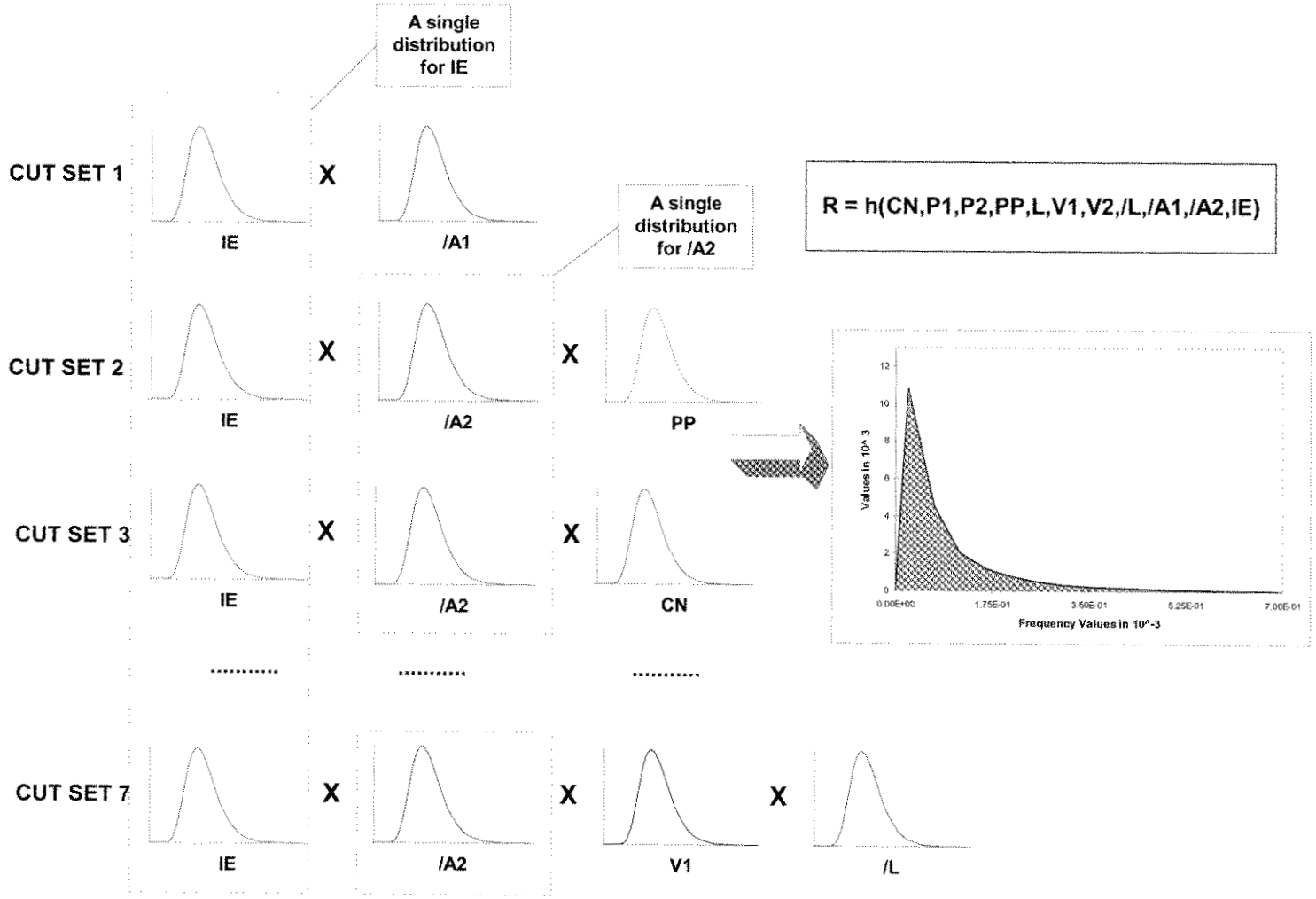
$$\Pr(CN) = 1 - e^{-\lambda_{CN} t}$$

  - **We use log normal distribution to characterize our uncertainty for λ_{CN}**
  - **Because λ_{CN} is uncertain, Pr(CN) would become uncertain.**
- **Each distribution defined in the right represents the *uncertainty in the occurrence probability of the event* as a result of uncertainty in the value of a parameter(s) that is used to generate the probability**

We assumed all events are log-normally distributed

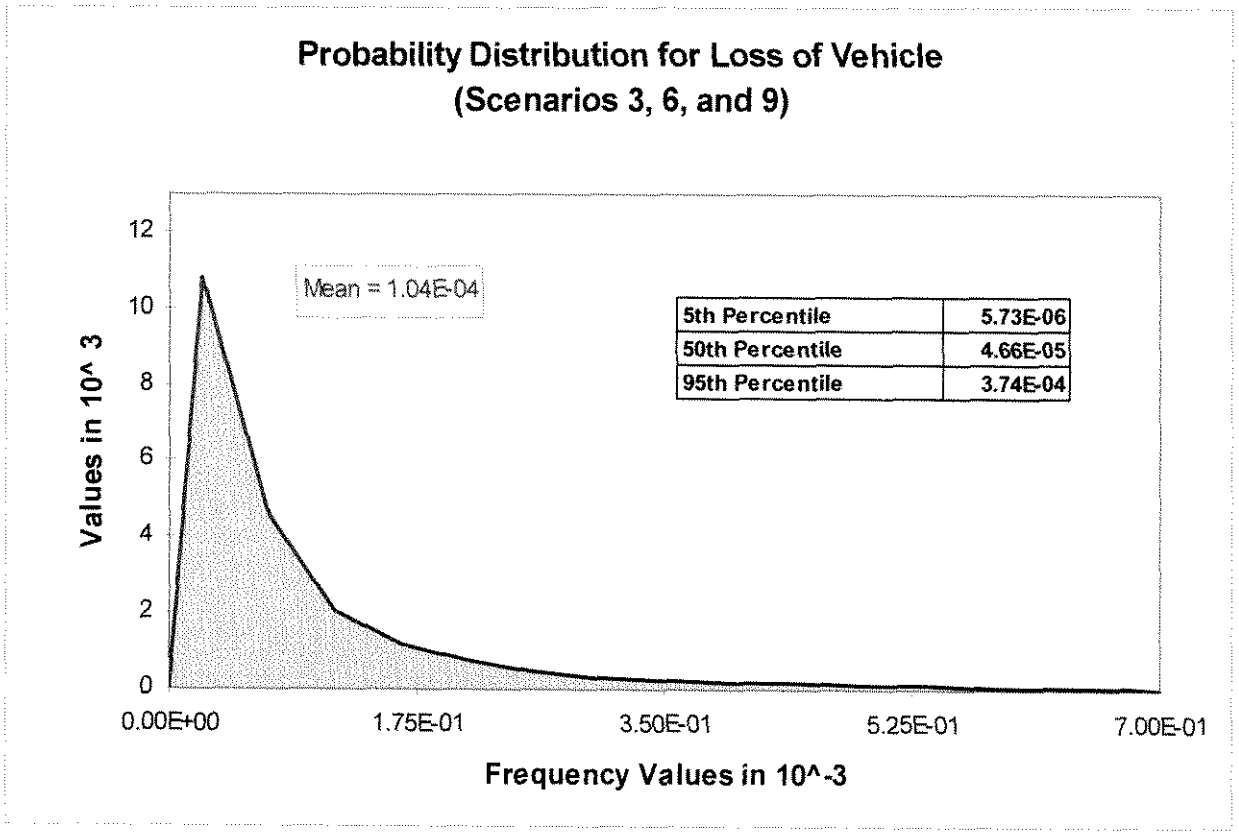
Event	Mean	EF
CN	1.00E-04	10
P1	1.00E-03	3
P2	1.00E-03	3
PP	1.00E-04	5
L	1.00E-01	3
V1	1.00E-03	3
V2	1.00E-03	3
/L	Dictated by L	
/A1	1.00E-05	5
/A2	1.00E-01	3
IE	1.00E-02	4

Uncertainty Propagation through the Model



Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Example of Risk Results



Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Insights

- **One scenario dominates the risk**
  - **leak occurs upstream of isolation valves. Because it is not isolable it can damage critical avionics**
  - **Contribution to risk: 97%**
- **Options to reduce risk**

	Structure of Dominant Scenario			
	IE: Leak occurs	**Leak occurs upstream of isolation valves**	**Leak damages critical avionics**	**Frequency**
OPTIONS	IE	L	/A2	
Do nothing	0.01	0.1	0.1	1.0E-4
Option 1: Reduce the likelihood of leak between the propellant tank and isolation valves (e.g., change in piping design)	0.01	0.05 (see note below)	0.1	5.0E-5
Option 2: Reduce susceptibility of avionics to leak (e.g., rerouting of wires and fortify wire harnesses)	0.01	0.1	0.01 (see note below)	1.0E-5
Option 1 and 2	0.01	0.05	0.01	5.0E-6
Note: The numerical values shown in this table are hypothetical.				

Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

Summary of PRA Strengths

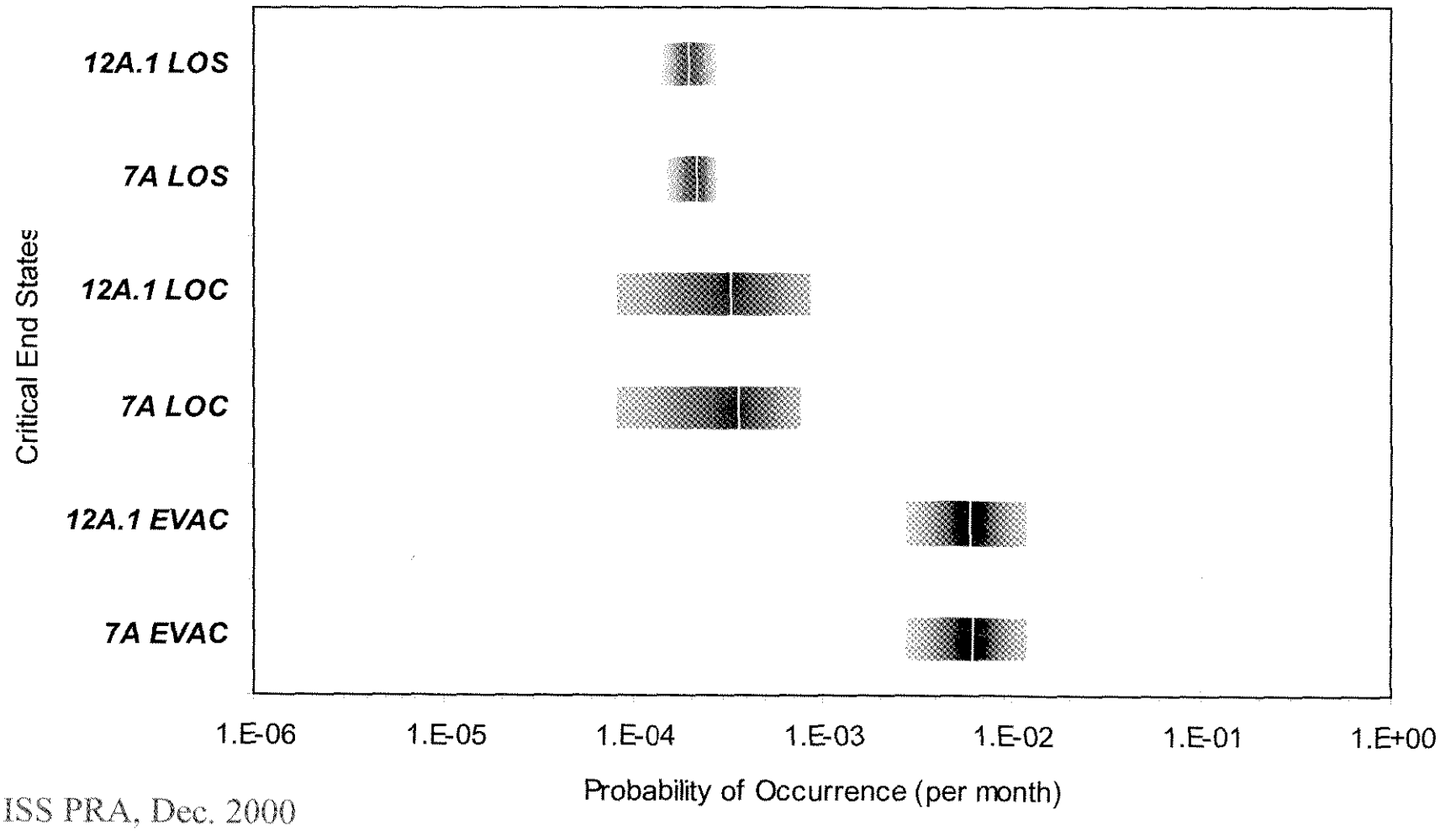
- Quantifies performance measures
  - Probability of Loss of Crew (LOC)
  - Probability of Loss of Mission (LOM)
  - PRA metrics are integral risk metrics
- Captures dependences and other relationships between sub-systems
- Works within a scenario-based concept of risk that best informs decision-making
  - Identifies contributing elements (initiating events, pivotal events, basic events)
  - Quantifies the risk significance of contributing elements, helping focus on where improvements will be effective
  - Provides a means of re-allocating analytical priorities according to where the dominant risk contributors appear to be coming from
  - Provides a framework for a monitoring / trending program to detect risk-significant adverse trends in performance

Summary of PRA Strengths (cont.)

- Quantifies uncertainty and ranks contributors to uncertainty
- Supports trade studies by quantifying
  - The most goal-related metrics
  - System interfaces and dependencies
  - Responses to system and function challenges
  - Effects of varying performance levels of different systems
- Can be a powerful tool when used to assist decision-making

PRA Results of a Real Space System

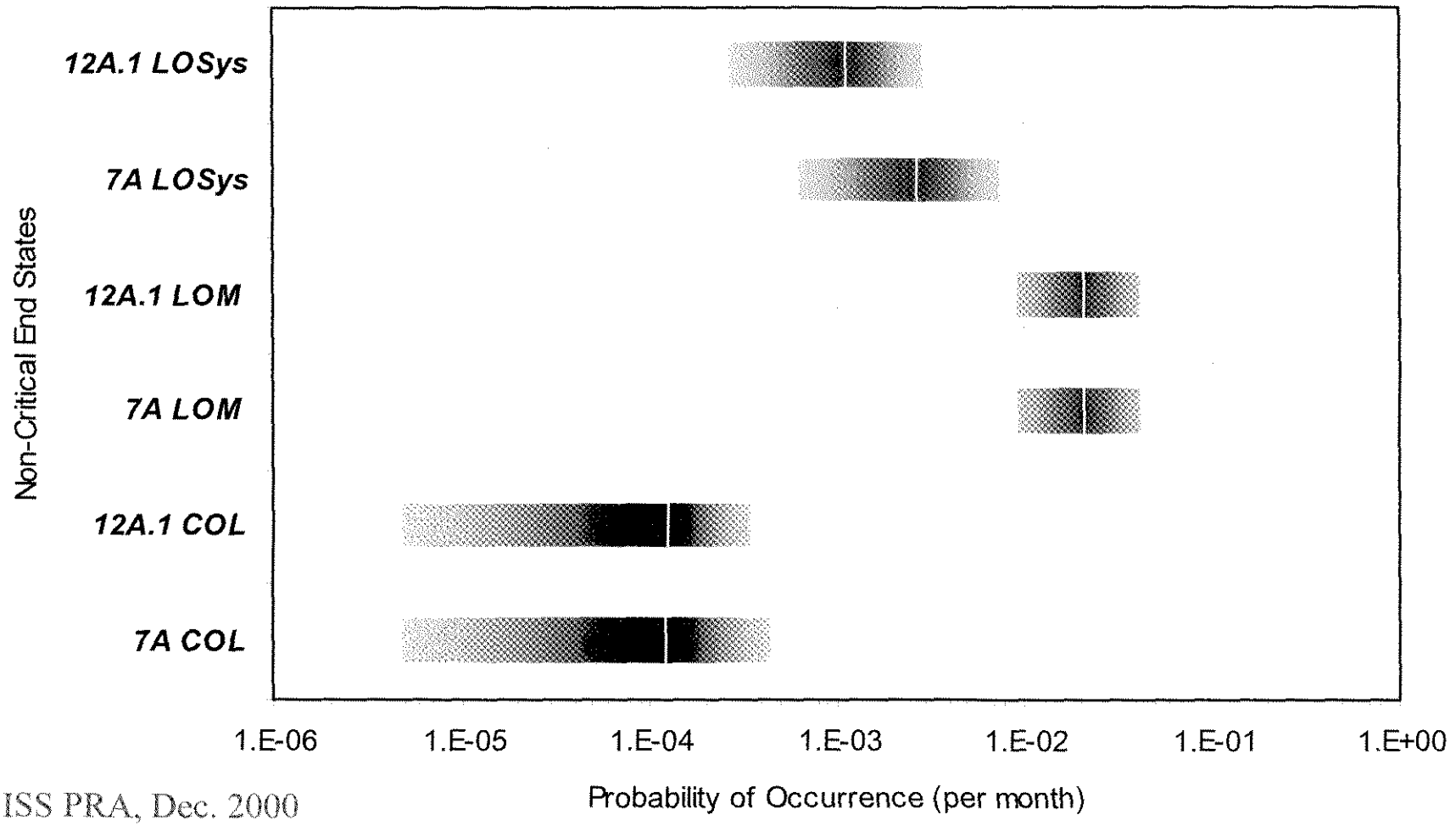
International Space Station (ISS) Critical End States



ISS PRA, Dec. 2000

Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

ISS Non-Critical End States

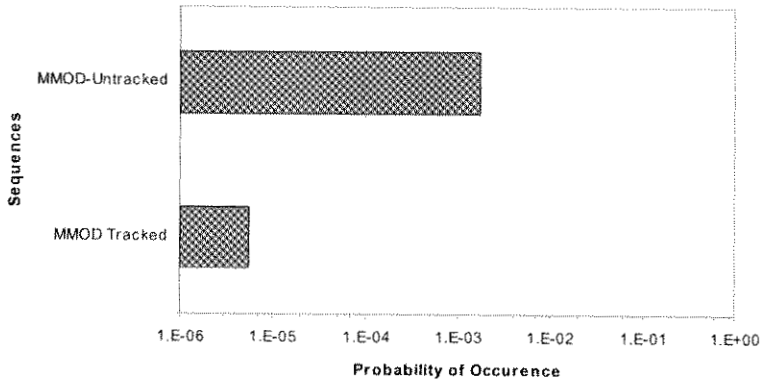


ISS PRA, Dec. 2000

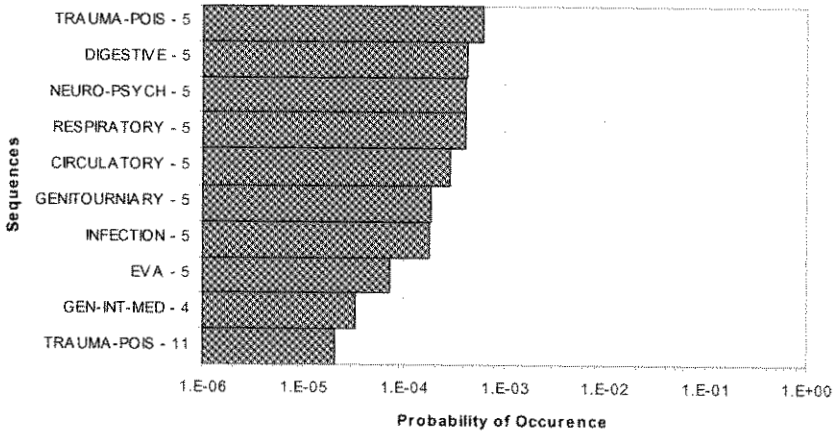
Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page

ISS Risk Drivers

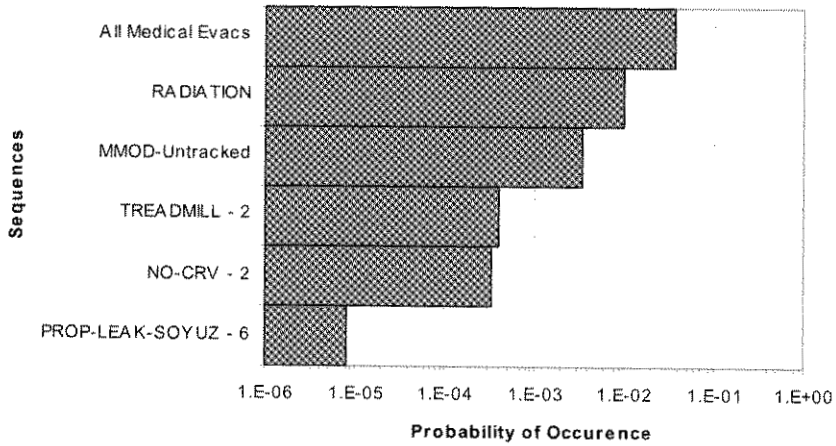
Loss of Station



Loss of Crew



ISS PRA, Dec. 2000



Evacuation

Presented by Homayoon Dezfuli, Ph.D.
Credit: See the acknowledgment statement on the first page